LANDesk® Management Suite 8

Benutzerhandbuch



Contents

Einführung in LANDesk® Management Suite 8 9

Neue Funktionen in LANDesk Management Suite 8 10

Verwendungsmöglichkeiten für Management Suite 8 12

Hier finden Sie weitere Informationen 13

Kapitel 1: Verwenden der LANDesk Management Suite-Konsole 15

Management Suite-Konsole - Übersicht 16

Starten der Management Suite-Konsole 31

Verwenden der rollenbasierten Administration 33

Konfigurieren der Agent-Erkennung 45

Anzeigen von Geräteeigenschaften 47

Überwachen von Clients aus Gründen der Netzwerkkonnektivität 49

Aktivieren des Core Server 51

Konfigurieren von Management Suite-Diensten 55

Kapitel 2: Konfigurieren der Clients 65

Client-Agent-Sicherheit und vertrauenswürdige Zertifikate 66

Erstellen einer Clientsetup-Konfiguration 70

Planen von Tasks 72

Konfigurieren lokaler Scheduler-Skripte 77

Verwenden von "Nicht verwaltete Geräteerkennung" 79

Verwenden von LANDesk Server Manager und LANDesk-Systemverwalter mit der LANDesk Management Suite 86

Ausführen des Client-Setup-Assistenten 88

Kapitel 3: Verwenden von Abfragen 113

Abfragenübersicht 114

Verwenden von Directory Manager für die Abfrage von Verzeichnissen über LDAP 118

Informationen über Lightweight Directory Access Protocol (LDAP) 122

Kapitel 4: Verwalten von Inventar und Berichten 125
Übersicht über das Inventarscannen 126
Anzeigen von Inventardaten 128
Verfolgen von Inventaränderungen 134
Verwenden von benutzerdefinierten Datenformularen 137
Übersicht über Berichte 143
Berichtsgruppen und vordefinierte Berichtslisten 144
Erstellen von benutzerdefinierten Inventarberichten 150
Kapitel 5: Fernverwaltung 153
Fernsteuerung von Clients 154
Konfiguration der Sitzungsoptionen 160
Ändern der Client-Fernsteuerungssicherheit 163
Konfigurieren der Mac OS X-Fernsteuerungsoptionen 164
Verwenden der Fernsteuerungsprotokollierung 165
Fehlerkorrektur bei Fernsteuerungssitzungen 166
Kapitel 6: Verteilen von Software und Dateien 169
Enhanced Software Distribution 170
Einrichten eines Paketerstellungscomputers 175
Übersicht über die Paketerstellung 176
Ausführen des Package Builder-Assistenten 179
Einrichten des Übermittlungsservers 181
Konfigurieren von Clients für den Empfang von Paketen 184
Verteilen eines Pakets 185
Arbeiten mit Mac OS X-Verteilungsskripten und -paketen 187
Verteilen von Dateien mit einem Dateiübertragungsskript 189
Deinstallieren von Softwareverteilungspaketen 190
Kapitel 7: Verwenden der Webkonsole 193
Info zur Webkonsole 193
Erste Schritte 195
Installieren und Konfigurieren von Clients 199
Verwalten von Inventardaten 202
Softwarelizenzüberwachung 211
Verteilen von Software und Dateien 223
Anpassen der Webkonsole 231
Tipps für die Fehlerkorrektur 238

Kapitel 8: Überwachen der Einhaltung von Softwarelizenzbestimmungen 241
Überwachen der Einhaltung von Softwarelizenzbestimmungen 242
Erstellen von Produkt- und Lieferantenaliasnamen.......................................243
Überwachung von Produkten hinsichtlich der Einhaltung von Lizenzbestimmungen 246
Bearbeiten des Softwareinventars 260
Exportieren und Importieren von Daten aus dem Fenster "Softwarelizenzüberwachung"..265
Verwenden der Softwarelizenzüberwachung mit Macintosh-Clients..................268
Kapitel 9: Verteilen von Betriebssystemabbildern und Migrieren von Profilen 271
Übersicht über die Betriebssystem-Verteilung 273
Richtlinien für Betriebssystemabbilder...275
Anpassen von Abbildern mit Sysprep und dem Installations-Manager 277
Agentbasierte Bereitstellung...279
Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten 280
Ändern von Skripts 283
Multicasting für Betriebssystemabbilder 284
Anzeigen von Abbildstatusberichten..286
PXE-basierte Bereitstellung 287
Verwenden von PXE-Repräsentanten 288
Starten von Clients mit PXE..290
Erläuterungen zu den PXE-Startoptionen 291
Übersicht über die Profilmigration 296
Profilinhalt 298
Erstellen von Migrationsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten 304
Erstellen von benutzerinitiierten Profilmigrationspaketen 306
Ausführen von benutzerinitiierten Profilmigrationspaketen 307

Kapitel 10: Reparieren von beschädigten Anwendungen 309
Konfigurieren von Application Healing 310
Konfigurieren von Schritt 1: Einrichten von ESWD-Paketen für die Reparatur 312
Konfigurieren von Schritt 2: Herstellen der Reparaturfähigkeit für Anwendungen 313
Konfigurieren von Schritt 3: Bereitstellen von ARL-Dateien auf Clients 317
Anzeigen von Application Healing-Ereignissen 319
Anzeigen von Application-Healing-Berichten 321
Application Healing-Registrierungsschlüssel 322
Kapitel 11: Verwalten von Anwendungsrichtlinien 325
Informationen über Application Policy Management 326
Konfigurieren von Richtlinien 328
Erläuterungen zu Richtlinientypen 332
Konfigurieren von Richtlinien auf Macintosh-Clients 333
Erstellen von Berichten über den Richtlinienstatus 335
Kapitel 12: Konfiguration von Alarmen zu Ihrer Benachrichtigung 337
Funktionsweise der Alarmfunktion in Management Suite 338
Konfigurieren von AMS-Alarmaktionen 339
Arbeiten mit konfigurierten Alarmaktionen 349
Anzeigen des AMS-Warnungsprotokolls 351
Kapitel 13: Verwenden des Patch Manager-Zusatzprodukts 355
Übersicht über Patch Manager 356
Informationen zum Patch Manager-Fenster 358
Konfigurieren von Clients für den Patch Manager 365
Aktualisieren von Anfälligkeits- und Erkennungsregelinformationen 369
Erstellen benutzerdefinierter Anfälligkeits- und Erkennungsregeln 374
Anzeigen von Anfälligkeits- und Erkennungsregelinformationen 380
Scannen von Clients auf Anfälligkeiten 390
Anzeigen erkannter Anfälligkeiten 392
Herunterladen von Patches 394
Reparieren von Anfälligkeiten 395
Verwenden von Patch Manager-Berichten 404

Kapitel 14: Verwenden des Zusatzprodukts zur Inventarverwaltung 407
Inventarverwaltung 407
Arbeiten mit Computerinventar 409
Arbeiten mit Softwareinventar 412
Verwalten von Verträgen 414
Verwalten von Rechnungen 415
Verwalten von Projekten 416
Verwalten von globalen Listen 417
Erstellen neuer Typen 419
Verwenden der Detailübersicht 421
Hinzufügen von Details 423
Hinzufügen von Tabellenfeldern 427
Verwalten von Detailvorlagen 429
Hinzufügen von Detailvorlagen 430
Verwenden einer Elementliste 431
Hinzufügen von Elementen zur Datenbank 432
Verknüpfen von Elementen 434
Importieren von Elementen 436
Exportieren von Elementen 438
Verwenden von Inventarverwaltungsberichten 440
Kapitel 15: Verwenden von LANDesk Inventory Manager 445
Benutzerdefinierte Formulare und Inventory Manager 446
Anhang A: Zusätzliche Inventaroperationen und Fehlerkorrektur 447
Scannen von benutzerdefinierten Daten 448
Festlegen von Intervall und Verlauf des Softwarescannens 449
Anhang B: Zusätzliche Informationen zur Betriebssystem-Verteilung und Profilmigration 463
Weitere Betriebssystem-Verteilungsverfahren 464
Verwenden des LANDesk-Abbildverarbeitungstools für DOS 472
Verwenden des LANDesk-Abbildverarbeitungstools für Windows 476

Anhang C: Zusätzliche Informationen zur Softwareverteilung 497
Skriptleitfaden für .CFG-Dateien 498
Fehlerkorrektur für .CFG-Dateien und ihre Pakete 506
Skriptleitfaden für Verteilungsskripts (.INI-Dateien) 508
Bedeutung der Enhanced Software Distribution-Fehlercodes 510
Dateien, die in Enhanced Software Distribution verwendet werden 514
Informationen über den Paketbereitstellungsassistenten 516

Einführung in LANDesk® Management Suite 8

LANDesk® Management Suite 8 enthält Tools zur Verwaltung Ihrer Windows NT*-, Windows* 2000/2003-, NetWare*-, Macintosh*-, Linux*- und UNIX*-Netzwerke. Mithilfe dieser Tools verteilen Sie Softwarepakete, überwachen die Verwendung von Software, stellen Betriebssystemabbilder bereit und migrieren Profile, steuern Clients fern und führen viele weitere Verwaltungstasks aus.

In diesem Kapitel erfahren Sie mehr über Management Suite 8. Es enthält unter anderem folgende Themen:

- Neue Funktionen in diesem Release
- Verwendungsmöglichkeiten für Management Suite 8
- Hier finden Sie weitere Informationen

Neue Funktionen in LANDesk Management Suite 8

- **Verbesserte Datenbank:** Neues Datenbankschema mit nur einer Datenbank sowie verbesserter Datenintegrität und Skalierbarkeit.
- **Rollenbasierte Administration:** Fügen Sie Management Suite-Benutzer hinzu und konfigurieren Sie ihre Zugriffsrechte auf Management Suite-Werkzeuge und Netzwerkgeräte basierend auf ihrer administrativen Rolle in Ihrem Netzwerk. In der rollenbasierten Administration weisen Sie Bereiche zu um festzulegen, welche Geräte bestimmte Benutzer anzeigen und verwalten können, sowie Berechtigungen um festzulegen, welche Tasks sie ausführen können. Siehe Rollenbasierte Administration in Kapitel 1.
- **Verbesserungen in Enhanced Software Distribution:** Zu den Verbesserungen gehören Checkpunkt-Neustarts auf Byte-Ebene bei unterbrochenen Downloads, Peer Download, dynamische Bandbreitendrosselung, die die Verteilungsbandbreite einschränkt, wenn Clients Netzwerkbandbreite benötigen, und Unterstützung für Multidatei-MSI-Multicast-Pakete. Siehe "Verwenden von Targeted Multicast mit Enhanced Software Distribution" und "Informationen zu Checkpunkt-Neustarts auf Byte-Ebene und dynamischer Bandbreitendrosselung" in Kapitel 6.
- **Neue Funktion "Nicht verwaltete Geräteerkennung":** Finden Sie unbekannte und nicht verwaltete Geräte in Ihrem Netzwerk über eine Verzeichnisdienst-, Domänenerkennungs- oder Schicht 3-Ping-Suche. Durch Warnmeldungen werden Sie auf Geräte hingewiesen, die neu entdeckt wurden. Planen Sie die Geräteerkennung, damit Sie immer über neue Geräte informiert werden. Siehe "Verwenden von "Nicht verwaltete Geräteerkennung"" in Kapitel 2.
- **Verbesserte Clientsicherheit:** Ein auf Zertifikaten basierendes Modell lässt Clients nur mit autorisierten Core Servern und Konsolen kommunizieren. Siehe "Client-Agent-Sicherheit und vertrauenswürdige Zertifikate" in Kapitel 2.
- **Neue Fernsteuerung auf Anforderung:** Optionales und äußerst sicheres Fernsteuerungsmodell auf Anforderung, mit dem der Fernsteuerungsagent nur für die Dauer der autorisierten Fernsteuerung auf Clients geladen wird. Siehe "Verteilen der Fernsteuerung" in Kapitel 2.
- **Neue Berichte:** Über 50 neue, vordefinierte Management Suite-Dienstberichte für die Planung und strategische Analysen. Siehe "Verwalten von Inventar und Berichten" in Kapitel 2.
- **Neue Konsolenoberfläche:** Neue Konsole mit verankerbaren Fenstern, Netzwerkansicht, benutzerdefinierten Layouts und vielem mehr. Siehe Kapitel 1 "Verwenden der LANDesk Management Suite-Konsole".
- **Zusätzliche Unterstützung für Macintosh-Computer:** Targeted Multicast, Application Policy Management und Softwarelizenzüberwachung für Mac OS * X-Clients. Siehe "Arbeiten mit Mac OS X-Verteilungsskripts und -paketen" in Kapitel 6, "Konfigurieren von Richtlinien für Macintosh-Clients" in Kapitel 11 und "Verwenden der Softwarelizenzüberwachung mit Macintosh-Clients" in Kapitel 8.

LANDesk Management Suite 8.1 wurde in folgenden Bereichen verbessert:

- **Verbessertes Inventar:** Sie können jetzt sofort einen Inventarscan auf einem Client starten, indem Sie mit der rechten Maustaste auf den Client und dann auf **Inventar** klicken. Der Inventarscanner sammelt jetzt auch die Daten zur Betriebssystemsprache auf Clients.
- **Verbesserte Softwareverteilung:** Die Softwareverteilung bietet jetzt eine bessere Unterstützung für Firewalls. Des Weiteren haben Sie jetzt die Möglichkeit, die Taskfertigstellung auf Softwareverteilungsaufträgen zu deaktivieren, sodass das nicht automatisch ein erneuter Ausführungsversuch durchgeführt wird, wenn ein Auftrag nicht ausgeführt werden konnte.
- **Verbesserte Webkonsole:** Erstellen Sie einfache Client-Konfigurationspakete und verwenden Sie die Softwarelizenzüberwachung vom Web aus. Siehe "Installieren von Clientagenten" und "Überwachen der Einhaltung von Softwarelizenzbestimmungen" in Kapitel 7.
- **Optimiertes Application Policy Management:** Jedes Mal, wenn ein Client den Core Server auf Tasks oder Richtlinien prüft, aktualisiert der Core Server die IP-Adresse des betreffenden Clients in der Core-Datenbank. Auf diese Weise werden Probleme mit veralteten IP-Adressen vermieden, die als Teil eines alten Inventarscans existieren können.
- **Verbesserte Unterstützung geplanter Tasks:** Stellen Sie mehrere für den Scheduler-Dienst zu authentifizierende Anmeldungen zur Verfügung, wenn Tasks auf Clients ausgeführt werden, auf denen keine Management Suite-Agenten installiert sind. Dies ist besonders für das Verwalten von Clients in mehreren Windows-Domänen von Nutzen. Siehe "Konfigurieren des Scheduler-Dienstes" in Kapitel 1.
- **Neue benutzerdefinierte Local Scheduler-Tasks:** Verwenden Sie den Local Scheduler der Management Suite auf Clients, um einen immer wiederholt auszuführenden Task per Fernsteuerung zu planen. Siehe "Konfigurieren lokaler Scheduler-Skripte" in Kapitel 2.
- **Verbesserte Fernsteuerung:** Speichern Sie detaillierte Fernsteuerungsprotokolle in der Datenbank. Die aufgezeichneten Informationen geben Auskunft darüber, welcher Benutzer die Fernsteuerungssitzung initiiert hat und welche Fernsteuerungstasks (Dateiübertragungen, Chat usw.) er auf dem Client ausgeführt hat. Als weitere Verbesserung gibt die Fernsteuerung jetzt auch dritten Maustasten-/Mausradbewegungen an Clients weiter. Siehe "Verwenden der Fernsteuerungsprotokollierung" in Kapitel 5.
- **Verbesserung der Funktion "Nicht verwaltete Geräteerkennung":** Erstellen Sie Berichte zu den nicht verwalteten Geräten in Ihrem Netzwerk. Um die Flexibilität zusätzlich zu verbessern, können Sie jetzt den Task "Nicht verwaltete Geräteerkennung" für die Wiedererkennung verwalteteter Clients verwenden. Dies ist von Nutzen, wenn Sie Ihre Datenbank zurückgesetzt haben. Siehe "Wiederherstellen von Clientdatensätzen" in Kapitel 2.
- **Neues LANDesk Asset Manager 8 Add-On:** Ermöglicht Ihnen die flexible Verwaltung Ihres physikalischen Inventars und die Durchführung von Inventar-Audits. Verfolgen Sie Verträge, Rechnungen und Bestellungen. Gleichen Sie das Vorhandensein und den Standort von IT-Inventarbeständen mit finanziellen Aufzeichnungen ab. Siehe Kapitel 14 "Verwenden des Add-On-Produkts zur Inventarverwaltung".
- **Verwenden des Patch Manager 8 Add-On:** Erstellen Sie benutzerdefinierte Anfälligkeiten, damit Sie Probleme schon erkennen, bevor ein Patch verfügbar ist. Sie können jetzt auch Mac OS X-Clients auf Anfälligkeiten scannen. Siehe Kapitel 13 "Verwenden des Patch Manager-Add-On".

Verwendungsmöglichkeiten für Management Suite 8

Management Suite 8 bietet Ihnen folgende Möglichkeiten:

- Verwenden der LANDesk Management Suite-Konsole zur Konfiguration und Verwaltung Ihres Netzwerkes. Siehe Kapitel 1 "Verwenden der LANDesk Management Suite-Konsole".
- Konfigurieren von Clients für Management Suite, Planen von Tasks und Erkennen von nicht verwalteten Clients. Siehe Kapitel 2 "Konfigurieren von Clients".
- Erstellen und Verwalten von Abfragen zu Inventardaten und LDAP-Verzeichnissen. Siehe Kapitel 3 "Verwenden von Abfragen".
- Verwalten von Inventaren, Verfolgen von Inventaränderungen, Erstellen von Formularen zum Sammeln benutzerdefinierter Daten von Clients und Anzeigen detaillierter Berichte. Siehe Kapitel 4 "Verwalten von Inventar und Berichten".
- Diagnose und Fehlerbehebung auf Fernclients von der Konsole aus. Sie können Fernclients steuern, neu starten, auf ihnen Dateien ausführen und Dateien an sie übertragen. Siehe Kapitel 5 "Fernverwaltung".
- Schnelles Verteilen von Software an alle Netzwerkbenutzer. Siehe Kapitel 6 "Verteilen von Software und Dateien".
- Verwenden einer webbasierten Konsole, um von jedem beliebigen Browser auf wichtige Management Suite-Funktionen zuzugreifen. Siehe Kapitel 7 "Verwenden der Webkonsole"
- Überwachen der Softwarelizenzen und der Einhaltung der Bestimmungen sowie Verfolgen der Softwareverwendung und der Verweigerungstrends. Außerdem Bearbeiten der Softwareliste der Core-Datenbank, LDAPPL3.INI, die der Inventarscanner zur Identifizierung von Client-Anwendungen verwendet. Siehe Kapitel 8 "Überwachen der Einhaltung von Softwarelizenzbestimmungen".
- Verteilen von Betriebssystemabbildern und Migrieren von Benutzerprofilen. Siehe Kapitel 9 "Verteilen von Betriebssystemabbildern und Migrieren von Profilen".
- Überwachen von Anwendungen auf Probleme und Reparieren von Anwendungen, wenn Probleme auftreten. Siehe Kapitel 10 "Reparieren von beschädigten Anwendungen".
- Erstellen von Anwendungsrichtlinien basierend auf Core-Datenbankabfragen. Clients, die Ziel einer Richtlinie sind, erhalten automatisch Anwendungssets. Siehe Kapitel 11 "Verwalten von Anwendungsrichtlinien".
- Einrichten von Alarmaktionen, durch die Sie benachrichtigt werden, wenn kritische Grenzwerte überschritten werden (z. B. Erhalt einer Pager-Nachricht, falls die Festplattennutzung 90 Prozent übersteigt). Siehe Kapitel 12 "Konfiguration von Alarmen zu Ihrer Benachrichtigung".

Hier finden Sie weitere Informationen

Im *LANDesk Management Suite Installations- und Verteilungshandbuch* finden Sie Informationen zu folgenden Themen:

- Systemanforderungen
- Installation von Management Suite
- Upgrades früherer Versionen von Management Suite
- Einrichten von Service Centers

Im *LANDesk Management Suite Benutzerhandbuch* finden Sie Informationen zu folgenden Themen:

- Verwenden der Konsole
- Konfigurieren von Diensten
- Einrichten von Clients
- Verteilen von Software und Dateien auf Clients
- Fernsteuerung von Clients
- Ermitteln von Hardware- und Softwareinventardaten
- Verteilen von Betriebssystemabbildern und Migrieren von Client-Profilen
- Verwalten von Patches
- Überwachen der Einhaltung von Softwarebestimmungen
- Verwaltung und Reparatur von Anwendungen
- Verwenden der Webkonsole
- Überwachen von Netzwerkservern
- Fehlerkorrektur

Kapitel 1: Verwenden der LANDesk Management Suite-Konsole

Die LANDesk Management Suite umfasst eine vollständige Sammlung von Werkzeugen, mit deren Hilfe Sie die Geräte im Netzwerk anzeigen, konfigurieren, verwalten und schützen können. Sie können alle diese Aktionen über die Management Suite-Konsole ausführen.

In diesem Kapitel erfahren Sie mehr über:

Verwenden der Management Suite-Konsole

- Management Suite-Konsole - Übersicht
- Erläuterungen zur Netzwerkansicht
- Starten der Management Suite-Konsole
- Ändern der Core Server-Verbindung
- Verwenden der rollenbasierten Administration
- Konfigurieren der Agent-Erkennung
- Anzeigen von Clienteigenschaften
- Überwachen von Geräten aus Gründen der Netzwerkkonnektivität
- Aktivieren des Core Server

Konfigurieren von Management Suite-Diensten

- Auswählen eines Core Servers und einer Datenbank
- Konfigurieren des Inventardienstes
- Konfigurieren des Scheduler-Dienstes
- Konfigurieren des Benutzerdefinierten Auftragsdienstes
- Konfigurieren des Multicast-Dienstes
- Konfigurieren des Betriebssystem-Verteilungsdienstes

Management Suite-Konsole - Übersicht

Der Vorteil der Management Suite-Konsole ist, dass Sie sämtliche Funktionen von einem Ort ausführen können und daher nicht mehr die verwalteten Clients einzeln aufsuchen müssen, um Routinewartungsarbeiten durchzuführen oder Fehler zu beheben. Von einer einzigen Konsole aus können Sie Software oder Konfigurationseinstellungen verteilen und aktualisieren, Hard- und Softwareprobleme diagnostizieren, Betriebssystemabbilder verteilen und Benutzerprofile migrieren, die rollenbasierte Administration zum Steuern des Zugriffs auf Funktionen und Geräte durch Benutzer der Management Suite verwenden und Fernsteuerungsfunktionen einsetzen, um Endbenutzer zu schulen oder um Probleme zu lösen.

Sie können über mehrere Core Server und Datenbanken verfügen, um Ihren individuellen Netzwerkverwaltungsanforderungen zu entsprechen. Informationen über die Installation eines LANDesk Management Suite-Core Servers und einer -Konsole, von zusätzlichen Konsolen, einer Webkonsole und die Verwaltung von mehreren Core Servern und Datenbanken finden Sie im *Installations- und Verteilungshandbuch* (dieses Handbuch steht als PDF-Dokument zur Verfügung, das ausgedruckt werden kann).

Im weiteren Verlauf dieses Kapitels erfahren Sie, wie Sie die neue LANDesk Management Suite 8-Konsole steuern und verwenden, um Geräte anzuzeigen und zu organisieren und auf die verschiedenen Verwaltungswerkzeuge zuzugreifen. (Management Suite-Werkzeuge, wie Software Distribution und Fernsteuerung, werden in den folgenden Kapiteln dieses Handbuchs beschrieben.)

- Erläuterungen zur Netzwerkansicht
- Erstellen von Gruppen
- Gerätesymbole
- Anzeigen der verwalteten Geräte in der Gruppe "Alle Geräte"
- Kontextmenüs
- Konfigurieren von Netzwerkansichtsspalten
- Symbolleistenoptionen
- Verwenden der Management Suite-Werkzeuge
- Verankerbare Fenster
- Automatisches Ausblenden
- Speichern von Fensterlayouts
- Suchleiste
- Statusleiste

Erläuterungen zur Netzwerkansicht

Die Netzwerkansicht ist das Hauptfenster der Management Suite-Konsole und der Ausgangspunkt für die meisten Funktionen. Hier können Sie die Inventardaten des Client anzeigen, Abfragen für die Suche und die Gruppierung von Geräten erstellen, Clients für die Fernsteuerung auswählen usw.

Das Fenster "Netzwerkansicht" ist stets geöffnet und besteht aus zwei Fensterausschnitten. Der linke Fensterausschnitt zeigt eine hierarchische Strukturansicht des Core Servers/der Datenbank, mit dem/der Sie gegenwärtig verbunden sind, sowie die entsprechenden Geräte, Abfragen und Konfigurationsgruppen. Sie können alle drei Strukturobjekte nach Bedarf erweitern oder reduzieren. Der rechte Fensterausschnitt der Netzwerkansicht zeigt eine detaillierte Liste der Geräte, Abfragen oder der Konfigurationselemente der ausgewählten Gruppen, abhängig von der Art der ausgewählten Gruppe.

Sie können das Fenster "Netzwerkansicht" und dessen Fensterausschnitte und Spalten vergrößern und verkleinern; Sie können es jedoch nicht schließen. Das Fenster "Netzwerkansicht" ist nicht verankerbar wie die Werkzeugfenster.

Rollenbasierte Administration
Als Benutzer der Management Suite ist die Frage, welche Geräte Sie in der Netzwerkansicht anzeigen und verwalten können und welche Verwaltungswerkzeuge Sie verwenden können, von den Zugriffsrechten und dem Gerätebereich ab, die Ihnen vom Management Suite-Administrator zugewiesen wurden. Weitere Informationen finden Sie unter "Rollenbasierte Administration" in diesem Kapitel.

Die Netzwerkstrukturansicht enthält die folgenden Gruppen und Untergruppen:

Core

Das Core-Objekt identifiziert den Core Server, mit dem Sie gegenwärtig verbunden sind. Das Core-Objekt befindet sich direkt unter dem Stamm der Netzwerkansicht und kann erweitert und reduziert werden. (Die Syntax für den Namen des Core-Objekts lautet: Servername\Datenbankinstanz.)

Geräte

Die Gruppe "Geräte" enthält die folgenden Geräteuntergruppen:

- **Eigene Geräte:** Führt die Geräte für die aktuell angemeldeten Benutzer auf, basierend auf dem Benutzerbereich. Ein Benutzer kann Geräteuntergruppen nur unter "Eigene Geräte" erstellen. Benutzer können Geräte zur Gruppe "Eigene Geräte" oder einer Untergruppe hinzufügen, indem Sie sie aus den Gruppen "Öffentliche Geräte" und "Alle Geräte" kopieren. Benutzer können auch Geräte unter "Öffentliche Geräte" und "Alle Geräte" anklicken und in die Gruppe "Eigene Geräte" ziehen.

Ziehen und Ablegen von Elementen in der Netzwerkansicht
Wenn Sie ein Element anklicken, um es in eine andere Gruppe in der Netzwerkansicht zu ziehen, zeigt der Cursor an, wo ein Ablegen möglich bzw. nicht möglich ist. Während Sie den Cursor über ein Gruppenobjekt ziehen, zeigt ein Pluszeichen (+) an, dass Sie das Element zu dieser Gruppe hinzufügen können und ein Durchgestrichenzeichen zeigt an, dass Sie das Element nicht zu dieser Gruppe hinzufügen können.

- **Öffentliche Geräte:** Führt Geräte, die ein Management Suite-Administrator aus der Gruppe "Alle Geräte" hinzugefügt hat. Ein Administrator (ein Benutzer mit LANDesk-Administratorrechten) kann alle Geräte in dieser Gruppe anzeigen, während andere Management Suite-Benutzer nur die Geräte sehen können, die zu ihrem Bereich gehören. Außerdem kann ein Administrator eine Untergruppe unter "Öffentliche Geräte" erstellen.
- **Alle Geräte:** Führt alle Geräte auf, die vom gegenwärtig angemeldeten Benutzer - basierend auf dessen Bereich - gesehen werden können - in einer Liste ohne Untergruppen. Für einen Administrator führt "Alle Geräte" alle verwalteten Geräte auf, die in die Core-Datenbank gescannt wurden. Geräte, auf denen Management Suite-Agenten (CBA und Inventar) ausgeführt werden, werden automatisch in der Gruppe/dem Ordner "Alle Geräte" angezeigt, wenn sie durch den Inventarscanner in die Core-Datenbank gescannt werden.

  Bei anderen Management Suite-Benutzern besteht "Alle Geräte" aus den "Eigenen Geräten" ihrer Benutzer und den Gruppen "Öffentliche Geräte".

  Administratoren und Benutzer können Anlagenberichte auf den Geräten in dieser Gruppe ausführen.
- **Benutzergeräte:** Führt alle Geräte in der Core-Datenbank auf, organisiert nach Benutzeruntergruppen. Benutzeruntergruppen werden mit den Benutzeranmelde-IDs benannt (d.h. Computername\Benutzerkonto oder Domäne\Benutzerkonto). Jede Benutzergruppe enthält die Geräte, die in der Gruppe "Eigene Geräte" dieses Benutzers angezeigt werden.

  Beachten Sie, dass NUR Administratoren die Gruppe "Benutzergeräte" und deren Untergruppen anzeigen können. Andere Benutzer können die Gruppe "Benutzergeräte" überhaupt nicht anzeigen.

Abfragen

Die Gruppe "Abfragen" enthält die folgenden Abfrageuntergruppen.

- **Eigene Abfragen:** Führt Abfragen auf, die entweder durch den gegenwärtig angemeldeten Benutzer erstellt oder durch einen Administrator zur Gruppe "Benutzerabfragen" eines Benutzers hinzugefügt wurden. Ein Benutzer kann Abfragegruppen und Abfragen unter der Gruppe "Eigene Abfragen" erstellen, ändern und löschen. Er kann auch Abfragen in diese Gruppe aus der Gruppe "Öffentliche Abfragen" kopieren.

  Jede Abfrage, die ein Benutzer ausführt, ist auf den Bereich der Geräte begrenzt, der durch den Benutzerbereich definiert ist. Wenn z. B. für einen Benutzer der Bereich "Alle Rechner" gilt, durchsucht die Abfrage alle Geräte in der Core-Datenbank; wenn der Benutzerbereich jedoch auf 20 Rechner begrenzt ist, werden nur 20 Rechner von der Abfrage durchsucht.

  Weitere Informationen über das Erstellen von Abfragen finden Sie unter "Erstellen von Datenbankabfragen" in Kapitel 3.

- **Öffentliche Abfragen:** Führt Abfragen auf, die ein Administrator oder ein Benutzer mit PQM (Public Query Management)-Recht hinzugefügt hat. Nur Benutzer, die entweder über LANDesk-Administrator- oder PQM-Rechte verfügen, können Abfragegruppen oder Abfragen in der Gruppe "Öffentliche Abfragen" hinzufügen, ändern oder löschen. Alle Benutzer können jedoch die Abfragen in dieser Gruppe sehen und sie in die Gruppe "Eigene Abfragen" kopieren.
- **Alle Abfragen:** Führt alle Abfragen auf, die vom gegenwärtig angemeldeten Benutzer - basierend auf dessen Bereich - gesehen werden können - in einer Liste ohne Untergruppen. "Alle Abfragen" bestehen aus der Gruppe "Eigene Abfragen" eines Benutzers und aus der Gruppe "Öffentliche Abfragen".
- **Benutzerabfragen:** Führt alle Abfragen in der Core-Datenbank auf, organisiert nach Benutzeruntergruppen. Benutzeruntergruppen werden mit ihren Anmelde-IDs benannt (d.h. Computername\Benutzerkonto oder Domäne\Benutzerkonto). Jede Benutzergruppe enthält die Abfragen, die in der Gruppe "Eigene Abfragen" dieses Benutzers angezeigt werden.

  Beachten Sie, dass NUR Administratoren die Gruppe "Benutzerabfragen" und deren Untergruppen anzeigen können. Andere Benutzer können die Gruppe "Benutzerabfragen" nicht anzeigen.

  Administratoren können diese Gruppe verwenden, um die Abfragen eines Benutzers im Bereich dieses Benutzers durchzuführen, als ob die Abfrage vom Benutzer selbst durchgeführt würde. Somit kann ein Administrator eine genaue Vorschau der Ergebnisse anzeigen, die auch ein Benutzer sieht, wenn er eine Abfrage ausführt.

Konfiguration

Die Gruppe "Konfiguration" enthält die folgenden Konfigurationsgeräte.

- **PXE-Warteschlange** Führt PXE-Warteschlangen und Clients auf, die sich in der PXE-Warteschlange befinden. Weitere Informationen finden Sie unter "Verwenden der PXE-Haltewarteschlange" in Kapitel 9.
- **Multicast-Domänenrepräsentanten:** Führt konfigurierte Multicast-Domänenrepräsentanten auf, die für den Softwareverteilungs-Belastungsausgleich verwendet werden können. Weitere Informationen finden Sie unter "Verwenden von Targeted Multicasting" in Kapitel 6.
- **PXE-Repräsentanten** Führt als PXE-Repräsentanten konfigurierte Clients auf, die Betriebssystemabbilder auf Clients in deren Subnetz verteilen können. Weitere Informationen finden Sie unter "Verwenden von PXE-Repräsentanten" in Kapitel 9.
- **Anstehende nicht verwaltete Clientverteilungen:** Führt Clients auf, die durch das Werkzeug "Nicht verwaltete Geräteerkennung" gefunden wurden und auf einen Clientkonfigurationsauftrag warten. Weitere Informationen finden Sie unter "Verwenden von "Nicht verwaltete Geräteerkennung"" in Kapitel 2.

Erstellen von Gruppen

Gruppen helfen Ihnen dabei, Geräte und Abfragen in der Netzwerkansicht der Konsole zu organisieren. Sie können Gruppen erstellen, um Netzwerkgeräte basierend auf der Funktion, der geographischen Lage, der Abteilung, dem Geräteattribut oder einer anderen Kategorie zu organisieren, die Ihren Anforderungen entsprechen. Sie können z. B. eine Marketinggruppe für alle Clients in der Marketingabteilung oder eine Gruppe erstellen, die alle Clients beinhaltet, auf denen ein bestimmtes Betriebssystem ausgeführt wird.

Richtlinien für das Erstellen von Gruppen

- **"Eigene Geräte" und "Eigene Abfragen":** Administratoren (Benutzer mit LANDesk-Administratorrechten) und alle anderen Management Suite-Benutzer können Gruppen unter "Eigene Geräte" und "Eigene Abfragen" erstellen.
- **Öffentliche Geräte:** Nur Administratoren können Gruppen unter "Öffentliche Geräte" erstellen.
- **Öffentliche Abfragen:** Nur Administratoren oder Benutzer mit PQM (Public Query Management-) Rechten können Gruppen unter "Öffentliche Abfragen" erstellen.
- **"Alle Geräte" und "Alle Abfragen":** Es gibt keine Untergruppen für "Alle Geräte" oder "Alle Abfragen". Benutzer, einschließlich Administratoren, können keine Gruppen unter "Alle Geräte" oder "Alle Abfragen" erstellen.
- **Benutzergeräte:** Nur Administratoren können Gruppen unter benutzerspezifischen Untergruppen in "Benutzergeräte" erstellen.
- **Benutzerabfragen:** Nur Administratoren oder Benutzer mit PQM (Public Query Management-) Rechten können Gruppen unter den benutzerspezifischen Untergruppen in "Benutzerabfragen" erstellen.

So erstellen Sie eine Gruppe

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf die übergeordnete Gruppe (wie z.B. **Eigene Geräte**). Klicken Sie dann auf **Neue Gruppe**. Wählen Sie alternativ die übergeordnete Gruppe und klicken Sie dann auf **Bearbeiten** | **Eigene Geräte** | **Neue Gruppe**.
2. Geben Sie einen Namen für die neue Gruppe ein und drücken Sie die **Eingabetaste**.

Sie können mit der rechten Maustaste auf Gruppen klicken, um verschiedene Tasks durchzuführen, basierend auf der Art der Gruppe. Wenn Sie beispielsweise eine Geräteuntergruppe erstellt haben, können Sie im Kontextmenü dieser Untergruppe auf folgende Optionen zugreifen:

- Geräte hinzufügen
- Erstellen einer neuen Untergruppe
- Ausführen eines Anlagenberichts
- Ausschneiden
- Kopieren
- Einfügen
- Umbenennen
- Entfernen

Weitere Informationen über die Funktionen, die durch Klicken mit der rechten Maustaste angezeigt werden, finden Sie nachfolgend unter Kontextmenüs.

Gerätesymbole

Gerätesymbole werden in der Netzwerkansicht der Konsole angezeigt und zeigen den gegenwärtigen Agenten und den Zustand des Geräts an.

Sie können Agent und Zustand jeweils für ein Gerät aktualisieren, wenn Sie es in der Netzwerkansicht auswählen, es können aber auch alle in der Netzwerkansicht angezeigten Geräte gleichzeitig aktualisiert werden. Sie können auch einen Gerätestatus aktualisieren, indem Sie ihn auswählen und in der Symbolleiste auf "Aktualisieren" klicken. Informationen zur Konfiguration der Agent-Erkennung finden Sie unter Konfigurieren von Agent-Erkennungsoptionen weiter unten in diesem Kapitel.

Die folgende Tabelle listet die möglichen Geräte- und Statussymbole sowie deren Bedeutung auf:

Symbol	Typ und Beschreibung
	Server: Stellt ein Servergerät dar.
	Windows-Client: Stellt einen Windows-Client dar.
	Macintosh-Client: Stellt einen Macintosh-Client dar.
	Handheld-Client: Stellt einen Handheld-Client dar.

Die folgenden Statussymbole können neben den oben bezeichneten Gerätesymbolen je nach der aktuellen Konfiguration und dem aktuellen Status angezeigt werden.

	Nicht verfügbar: Zeigt an, dass das Gerät gegenwärtig nicht für die Konsole zur Verfügung steht.
	Unbekannt: Zeigt an, dass der Status des Geräts gegenwärtig nicht bekannt ist. Dieses Symbol wird kurz angezeigt, während der Gerätestatus aktualisiert wird.
	CBA: Zeigt an, dass der Common Base Agent (CBA) auf dem Client geladen ist.

Fernsteuerung: Zeigt an, dass der Fernsteuerungsagent auf dem Client geladen ist.

Warnung: Gibt eine Zustandswarnung für den Client an. Ein Zustandssymbol wird nur dann angezeigt, wenn der LANDesk System Manager-Agent auf dem Client geladen ist.

Kritisch: Gibt einen kritischen Zustand für den Client an. Ein Zustandssymbol wird nur dann angezeigt, wenn der LANDesk System Manager-Agent auf dem Client geladen ist.

Symbolanzeigequalität
Es handelt sich um High-Color-Symbole, für die mindestens eine Farbtiefeneinstellung von 16 Bit erforderlich ist. Wenn die Symbole in der Konsole nicht fokussiert dargestellt werden, ändern Sie die Farbeinstellungen unter "Eigenschaften von Anzeige".

Wenn Ihre Firewall, UDP-Pakete blockiert
Wenn Sie Clients über eine Firewall verwalten, die UDP-Pakete blockiert, können Sie die folgenden Funktionen des Client-Kontextmenüs nicht verwenden: **Reaktivieren**, **Herunterfahren**, **Neustart** und **Inventarscan**.

Anzeigen der verwalteten Geräte in der Gruppe "Alle Geräte"

Geräte, auf denen Management Suite-Agenten (CBA und Inventar) ausgeführt werden, werden automatisch in der Gruppe "Alle Geräte" angezeigt, wenn sie durch den Inventarscanner in die Core-Datenbank gescannt werden. In der Regel wird dieser Scan zum ersten Mal während der ersten Clientkonfiguration durchgeführt. Wenn ein Client in die Core-Datenbank gescannt wurde, wird er als verwalteter Client betrachtet. Anders gesagt kann er nun durch diesen Core Server verwaltet werden. Weitere Informationen zum Einrichten von Clients finden Sie in Kapitel 2 "Konfigurieren von Clients".

Da die Gruppe "Alle Geräte" automatisch über einen Inventarscan gefüllt wird, müssen Sie möglicherweise nie manuell nach Clients suchen. Um jedoch Clients zu finden, die nicht bereits in der Core-Datenbank sind, können Sie das Netzwerks nach Clients mithilfe des Werkzeugs "Nicht verwaltete Geräteerkennung" durchsuchen. Weitere Informationen finden Sie unter "Verwenden von "Nicht verwaltete Geräteerkennung"" in Kapitel 2.

Wenn eine Verbindung zu einem bestimmten Core Server besteht, kann der Management Suite-Administrator jeden Client sehen, der von diesem Core Server verwaltet wird. Benutzer der Management Suite sind andererseits eingeschränkt und können nur die Clients sehen, die zu ihrem zugewiesenen Bereich gehören (ein Bereich basiert auf einer Datenbankabfrage oder einem Verzeichnisstandort). Weitere Informationen finden Sie unter "Verwendung der rollenbasierten Administration" weiter unten in diesem Kapitel.

Kontextmenüs

Die Kontextmenüs (Kurzbefehlmenüs) wurden in LANDesk Management Suite 8 für alle Elemente in der Konsole, einschließlich Gruppen, Geräte, Abfragen, geplante Tasks, Skripts, Berichte usw., erheblich erweitert. Kontextmenüs ermöglichen den schnellen Zugriff auf die allgemeinen Tasks und wichtige Informationen eines Elements.

Sie können das Kontextmenü eines Elements anzeigen, indem Sie das Element auswählen und mit der rechten Maustaste darauf klicken.

Wenn Sie beispielsweise in der Netzwerkansicht mit der rechten Maustaste auf einen verwalteten Client klicken, zeigt dessen Kontextmenü in der Regel die folgenden Optionen an:

- **Inventar:**Zeigt alle in die Core-Datenbank gescannten Inventardaten des Clients an.
- **Inventarverlauf:**Zeigt Änderungen der Inventardaten für die Attribute an, die Sie für das Verfolgen ausgewählt haben. Sie können den Inventarverlauf drucken oder in eine CSV-Datei exportieren.
- **Fernsteuerung:**Öffnet eine Fernsteuerungssitzung mit dem Client.
- **Chat:**Öffnet eine Remote-Chat-Sitzung mit dem Client.
- **Dateiübertragung:**Öffnet das Dialogfeld "Dateiübertragung", in dem Sie Dateien auf und vom Client übertragen können.
- **Fernausführung:**Hiermit können Sie eine Stapeldatei oder eine Anwendung suchen und sie auf dem Client ausführen
- **Reaktivieren:**Reaktiviert über Fernzugriff einen Client, dessen BIOS die Wake on LAN*-Technologie unterstützt.
- **Herunterfahren:**Fährt über Fernzugriff den Client herunter.
- **Neustart:**Startet über Fernzugriff den Client neu.
- **Inventarscan:**Führt einen Inventarscan auf dem Client aus.
- **Zu neuer Gruppe hinzufügen:**Fügt eine Kopie des Client in eine neue benutzerdefinierte Gruppe unter der Gruppe "Eigene Geräte" ein. Sie werden aufgefordert, einen Namen für die neue Gruppe einzugeben.
- **Zur vorhandenen Gruppe hinzufügen:** Damit können Sie die Gruppe auswählen, in die Sie eine Kopie des Client hinzufügen möchten.
- **Geplante Tasks und Richtlinien:** Zeigt die aktuellen geplanten Tasks des Client und Anwendungsverwaltungsrichtlinien an.
- **Gruppenmitgliedschaft:**Zeigt alle Gruppen an, denen der Client gegenwärtig angehört.
- **Anlagenbericht ausführen:**Öffnet das Dialogfeld "Berichte". In diesem Dialogfeld können Sie aus einer Liste von Anlagenberichten die auf dem Client auszuführenden Berichte auswählen können. Doppelklicken Sie auf den Bericht, um ihn auszuführen.
- **Service Center:**Öffnet den Service Center-Assistenten, den Sie zur Installation und Konfiguration eines Service Center verwenden können, um den Belastungsausgleich zu unterstützen.
- **Ausschneiden:Entfernt** Elemente aus einer benutzerdefinierten Gruppe. Sie können keine Elemente aus den Gruppen "Alle" ausschneiden.
- **Kopieren:**Erstellt eine Kopie des Elements, das Sie zu einer anderen Gruppe hinzufügen können.
- **Einfügen:**Platziert das Element, das Sie ausgeschnitten oder kopiert haben, in einer benutzerdefinierte Gruppe.

- **Entfernen:**Entfernt das Element aus einer benutzerdefinierten Gruppe.
- **Delete:**Löscht das Element aus der Gruppe "Alle" UND aus allen anderen Gruppen, in denen es gegenwärtig Mitglied ist.
- **Eigenschaften: Zeigt** die Inventarzusammenfassung des Clients, Geräteinformationen, Agentenstatus und Fernsteuerungseinstellungen an.

Dieses Handbuch beinhaltet nicht das Kontextmenü jedes Konsolenelements. Wir empfehlen Ihnen jedoch, dass Sie auf ein beliebiges Element mit der rechten Maustaste klicken, um die verfügbaren Optionen anzuzeigen.

Konfigurieren von Netzwerkansichtsspalten

Über "Spaltenkonfigurationen" können Sie Inventardaten anpassen, die in der Netzwerkansicht angezeigt werden. Sie können auch die Schaltfläche **Spalten auswählen** des Abfrage-Dialogfeldes verwenden, um festzulegen, wie Abfrageergebnisse in der Netzwerkansicht angezeigt werden. Spaltenkonfigurationen werden auch verwendet, um den Inhalt von Inventaranlagenberichten zu bestimmen.

So wenden Sie eine Spaltenkonfiguration auf die Netzwerkansicht an

1. Klicken Sie auf **Konfigurieren | Spalten**.
2. Wählen Sie eine Spaltenkonfiguration aus der Liste aus.
3. Klicken Sie auf **Schließen und übernehmen**, um die ausgewählte Spaltenkonfiguration auf den rechten Fensterausschnitt der Netzwerkansicht anzuwenden.

Informationen zum Dialogfeld "Spaltenkonfigurationen verwalten"

Verwenden Sie dieses Dialogfeld, um eine Spaltenkonfiguration auszuwählen und die Geräteinventardaten festlegen, die in der Netzwerkansicht angezeigt werden.

- **Spaltenkonfigurationen:** Listet alle verfügbaren Spaltenkonfigurationen nach Namen auf.
- **Neu:** Öffnet das Dialogfeld "Spaltenkonfiguration", in dem Sie eine neue Spaltenkonfiguration erstellen können.
- **Löschen:** Entfernt die ausgewählte Spaltenkonfiguration aus der Liste.
- **Eigenschaften:** Öffnet das Dialogfeld "Spaltenkonfiguration", in dem Sie eine neue Spaltenkonfiguration erstellen können.
- **Umbenennen:** Definiert das Namensfeld als definierbar, sodass Sie einen anderen Namen eingeben können.
- **Schließen und übernehmen:** Schließt das Dialogfeld und wendet die ausgewählte Spaltenkonfiguration auf Gerätelisten in der Netzwerkansicht an.
- **Schließen:** Schließt das Dialogfeld, ohne die aktuelle Spaltenkonfiguration zu ändern.

Spaltenkonfigurationen erstellen Sie im Dialogfeld "Spaltenkonfiguration". Jede Spalte stellt ein einzelnes Inventarattribut dar, das in die Core-Datenbank gescannt wird. Spalten werden von links nach rechts in der Netzwerkansicht in der Reihenfolge angezeigt, in der sie in der Liste "Spalten" zu sehen sind.

So erstellen Sie eine Spaltenkonfiguration

1. Klicken Sie auf **Konfigurieren | Spalten**.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Dialogfeld "Spaltenkonfiguration" einen Namen für die neue Spaltenkonfiguration ein.
4. Wählen Sie Inventarattribute aus der Liste aus und fügen Sie sie zur Liste "Spalten" hinzu, indem Sie auf **Zu Spalten hinzufügen** klicken.
5. Wenn Sie möchten, können Sie das Erscheinungsbild der Spalten anpassen, indem Sie die Attributüberschrift umbenennen, nach oben oder unten in der Liste verschieben oder entfernen.
6. Klicken Sie auf **OK**, um die Spaltenkonfiguration zu speichern.

Informationen über das Dialogfeld "Spaltenkonfigurationen"

Mithilfe dieses Dialogfeldes erstellen Sie eine neue Spaltenkonfiguration.

- **Name:** Identifiziert die Spaltenkonfiguration.
- **Inventarattribute:** Listet alle Inventarobjekte und die Attribute auf, die in die Core-Datenbank gescannt wurden. Sie können Objekte erweitern oder reduzieren, indem Sie auf das Feld auf der linken Seite jedes Objekts klicken.
- **Zu Spalten hinzufügen:Verschiebt das ausgewählte Inventarattribut in die Spaltenliste. Wenn Sie eine ganze Inventarkomponente wählen, werden alle Inventarattribute in dieser Komponente zur Liste "Spalten" hinzugefügt.**
- **Spalten:** Führt die Inventarattribute in der Reihenfolge auf, in der sie in der Netzwerkansicht angezeigt werden; von links nach rechts.
- **Umbenennen:** Damit können Sie den Attributnamen bearbeiten. Dieser Name wird in der Spaltenüberschrift angezeigt.
- **Entfernen:** Entfernt das ausgewählte Attribut aus der Liste.
- **Nach oben:** Verschiebt das ausgewählte Attribut um eine Position nach oben.
- **Nach unten:** Verschiebt das ausgewählte Attribut um eine Position nach unten.
- **OK:** Speichert die aktuelle Spaltenkonfiguration und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Symbolleistenoptionen

Die Management Suite-Konsole umfasst eine Symbolleiste, die einen Zugriff durch nur einen Klick auf die allgemeine Netzwerkansicht und einige grundlegende Konsolenkonfigurationsoptionen ermöglicht. Die Symbolleistenschaltflächen sind abgeblendet, wenn ein Element in der Netzwerkansicht ausgewählt ist, das diesen Vorgang nicht unterstützt.

Sie können Textbeschreibungen für die Symbolleistenschaltflächen aktivieren, indem Sie auf **Ansicht | Symbolleistentext anzeigen** klicken.

Die Konsolensymbolleiste umfasst die folgenden Schaltflächen:

- **Ausschneiden:** Entfernt Elemente aus der "Netzwerkansicht" und speichert sie temporär in der Zwischenablage. Wenn Sie versehentlich ein Element ausschneiden, verwenden Sie die Funktion "Einfügen", um es wiederherzustellen. Sie müssen das gelöschte Element wiederherstellen, bevor Sie einen anderen Befehl ausführen.
- **Kopieren:** Kopiert Elemente von einem Speicherort in der Netzwerkansicht in einen anderen.
- **Einfügen:** Fügt Elemente ein, die Sie ausgeschnitten oder kopiert haben.
- **Löschen:** Löscht das Element permanent. Sie können keine Elemente wiederherstellen, die Sie aus der Netzwerkansicht gelöscht haben.
- **Aktualisieren:** Aktualisiert die ausgewählte Gruppe oder das Element in der Netzwerkansicht. Sie können eine Gruppe auch reduzieren und erweitern, um die Elemente zu aktualisieren. Sie können auch auf **Ansicht | Aktualisieren** klicken, um das gegenwärtig in der Netzwerkansicht ausgewählte Element zu aktualisieren.
- **Layout:** Führt Ihre gespeicherten Fensterlayouts auf. Wählen Sie ein Layout aus der Dropdownliste aus, um die Konsole auf diese Layoutkonfiguration wiederherzustellen. Wenn Sie das gegenwärtige Layout speichern möchten, klicken Sie auf die Schaltfläche **Speichern**.
- **Core:** Führt verfügbare Core Server auf, zu denen Sie eine Verbindung herstellen können. Sie können einen Core Server aus der Liste auswählen oder den Namen eines Core Servers eingeben und die **Eingabetaste** drücken. Die Management Suite sucht nach dem Core Server auf dem Netzwerk und fordert Sie zur Anmeldung mit einem gültigen Benutzernamen und Kennwort auf.

Verwenden der Management Suite-Werkzeuge

Die Management Suite-Werkzeuge sind sowohl über das Menü "Extras" als auch über die Toolbox verfügbar. Um die Toolbox zu aktivieren, klicken Sie auf **Ansicht | Toolbox**.

Ein Administrator sieht alle Werkzeuge sowohl im Menü "Extras" als auch in der Toolbox. Andere Management Suite-Benutzer sehen nur die Werkzeuge (Funktionen), die durch die zugewiesenen Rechte zugelassen sind. Werkzeuge, die auf Rechten basieren, die einem Benutzer nicht gewährt wurden, werden weder im Menü "Extras" noch in der Toolbox angezeigt, wenn ein Benutzer an der Konsole angemeldet ist. Wenn ein Benutzer z. B. nicht über das Berichtsrecht verfügt, wird das Werkzeug "Berichte" weder im Menü "Extras" noch in der Toolbox angezeigt.

Hier finden Sie eine vollständige Liste der Management Suite-Werkzeuge:

- **Application Healing:** Sorgt dafür, dass Anwendungen funktionsfähig bleiben durch automatische Reparaturen von festgelegten Anwendungen.
- **Application Policy Management:** Verwaltet Anwendungssätze auf Gruppen von Clients.
- **Clientsetup:** Konfiguriert Clients mit LANDesk-Agenten, um ihre vollständige Verwaltbarkeit sicherzustellen.
- **Benutzerdefinierte Datenformulare:** Sammelt benutzerdefinierte Daten von Benutzern und fügt sie der Core-Datenbank hinzu.
- **Directory Manager:** Fragt LDAP-Verzeichnisse nach Clients ab.

- **Skripts verwalten:** Verwaltet Betriebssystem-Verteilung und Profilmigrationsskripts, Verteilungsskripts, Dateiübertragungsskripts und andere benutzerdefinierte Skripts.
- **PXE-Startmenü:** Konfiguriert das Startmenü, das auf PXE-Clients beim ersten Starten angezeigt wird.
- **Berichte:** Verwaltet vordefinierte LDMS-Dienste und Anlagenberichte und ermöglicht Ihnen die Erstellung Ihrer eigenen benutzerdefinierten Anlagenberichte.
- **Geplante Tasks:** Plant Clientkonfiguration, Software-Paketverteilung, Betriebssystem-Verteilung und Profilmigration sowie weitere Verwaltungstasks.
- **Softwarelizenzüberwachung:** Implementiert die Softwareinventarverwaltung und Lizenzerfüllungsrichtlinien.
- **Nicht verwaltete Geräteerkennung:** Sucht nach Clients im Netzwerk, die nicht in die Core-Datenbank gescannt wurden
- **Benutzer:** Steuert den Management Suite-Benutzerzugriff auf Geräte und Werkzeuge basierend auf den Rechten und dem Bereich des Benutzers.

Wenn Sie auf einen Werkzeugnamen klicken, wird das Werkzeugfenster in der Konsole geöffnet. Werkzeugfenster können vergrößert/verkleinert, verankert, unverankert, ausgeblendet und geschlossen sein. Sie können mehrere Werkzeugfenster gleichzeitig geöffnet haben, verankert oder unverankert. Weitere Informationen über das Steuern von Werkzeugfenstern finden Sie im nächsten Abschnitt.

Verankerbare Werkzeugfenster

Verankerbare Fenster sind eine Funktion der Konsolenbenutzeroberfläche, mit deren Hilfe Sie beliebig viele Management Suite-Werkzeuge öffnen können und sie in und aus das/dem Hauptkonsolenfenster schieben können.

Hinweis: Sie können ein Konsolenlayout, das Sie erstellt haben und für bestimmte Verwaltungstasks verwenden möchten, speichern und ein gespeichertes Layout jederzeit wiederherstellen, wenn Sie es benötigen. Weitere Informationen finden Sie unter "Speichern von Fensterlayouts" weiter unten in diesem Kapitel.

Wenn Sie mehrere Werkzeugfenster öffnen, werden sie mit Registerkarten in einem Fenster angezeigt. Das aktive Werkzeugfenster wird oben angezeigt und für jedes geöffnete Werkzeug wird entlang der Seite oder Unterseite eine Registerkarte für jedes geöffnete Werkzeug angezeigt. Klicken Sie auf eine Registerkarte, um das betreffende Werkzeugfenster anzuzeigen. Das Werkzeugfenster mit den Registerkarten lässt sich ziehen, sodass es außerhalb des Konsolenfensters unverankert angezeigt wird.

Ein Werkzeugfenster zu verankern bedeutet, es an eine der Kanten der Konsole anzuhängen. Das Fenster gilt als verankert, wenn es gegenwärtig an einer Ecke der Konsole angehängt ist. Sie können auch die Verankerung des Werkzeugfensters aufheben und es außerhalb der Konsole unverankert anzeigen lassen. Sie können Fenster waagrecht oder senkrecht in der Konsole verankern.

So verankern Sie ein Werkzeugfenster

1. Klicken Sie auf die Titelleiste eines Fensters und ziehen Sie das Fenster an eine Kante der Konsole.
2. Wenn das Verankerungsrechteck (abgeblendete Kontur des Fensters) angezeigt wird und angibt, dass das Fenster verankert wird, lassen Sie die Maustaste los. Das Fenster wird an diese Ecke der Konsole angehängt.

Beachten Sie, dass nur Werkzeugfenster (über das Menü "Extras" oder die Toolbox verfügbare Fenster) verankert, unverankert oder mit Registerkarten ausgestattet sein können. Das Fenster "Netzwerkansicht" kann vergrößert/verkleinert werden; es kann jedoch keine anderen Fenster als Registerkarten beinhalten, unverankert außerhalb der Konsole sein oder geschlossen werden.

Wenn Sie das Hauptfenster der Konsole verkleinern und dann wiederherstellen, werden bei diesem Vorgang alle verankerten und unverankerten Fenster, einschließlich der Fenster mit Registerkarten, ebenfalls verkleinert und wiederhergestellt.

Automatisches Ausblenden

Das Werkzeugfenster unterstützt außerdem die Funktion zum automatischen Ausblenden. Diese Funktion ist über eine Pin-Schaltfläche in der oberen rechten Ecke eines Fensters verfügbar, mit deren Hilfe ein Fenster an seiner Position gehalten oder ausgeblendet wird.

Wenn der Pin drinnen ist (d.h. der Pin nach unten zeigt), verbleibt das Fenster an seinem Platz und das automatische Ausblenden ist vorübergehend deaktiviert. Wenn der Pin draußen ist (d.h. der Pin nach links zeigt), wird das Fenster automatisch ausgeblendet, wenn sich der Cursor nicht mehr über dem Fenster befindet. Durch das automatische Ausblenden wird das Fenster verkleinert und an den Kanten der Konsole verankert, wo es als Registerkarte angezeigt wird.

Die Toolbox unterstützt ebenfalls das automatische Ausblenden.

Speichern von Fensterlayouts

Layouts sind gespeicherte Konsolenkonfigurationen, einschließlich der Position und der Größe des Fensters "Netzwerkansicht", der Toolbox und aller geöffneten Werkzeugfenster. Sie können Fensterlayouts verwenden, um benutzerdefinierte Konsolenkonfigurationen zu speichern und wiederherzustellen, die besonders hilfreich für bestimmte Benutzertasks sind.

Um das Layout der Konsole zu ändern, wählen Sie ein gespeichertes Layout aus der Dropdownliste **Layout** in der Hauptsymbolleiste aus.

So speichern Sie das gegenwärtige Layout

1. Konfigurieren Sie die Benutzeroberfläche der Konsole nach Ihren Bedürfnissen.
2. Klicken Sie in der Symbolleiste auf das Symbol **Diskette** neben der Dropdownliste **Layout**.
3. Geben Sie einen eindeutigen Namen für das Layout ein.
4. Klicken Sie auf **OK**.

Info über das Dialogfeld "Fensterlayouts verwalten"

Verwenden Sie dieses Dialogfeld zum Verwalten von gespeicherten Fensterlayouts und zum Zurücksetzen des Konsolenfensters auf das vorherige Layout.

- **Gespeicherte Layouts:** Führt alle Ihre gespeicherten Layouts auf.
- **Zurücksetzen:** Stellt das vorherige Layout des Konsolenfensters wieder her.
- **Löschen:** Entfernt das ausgewählte Layout.
- **Umbenennen:** Damit können Sie den Namen des ausgewählten Layouts ändern.

Suchleiste

Mit "Suchen" können Sie nach Elementen in einer Liste suchen, die ein bestimmtes Wort oder eine Phrase enthält. Die Suchleiste ist in der Netzwerkansicht und in Werkzeugfenstern verfügbar, die Elementlisten enthalten. Die Suchleiste erscheint z. B. bei der Anzeige von:

- Gruppe "Alle Geräte"
- Gruppe "Alle Abfragen"
- Gruppe "Anstehende nicht verwaltete Clientverteilungen"
- Werkzeugfenster "Nicht verwaltete Geräteerkennung"
- Alle Anlagenberichte

So suchen Sie nach einem Element mithilfe der Suchleiste

1. Wählen Sie die Gruppe **Alle Geräte**. Die Suchleiste wird am Beginn der Liste angezeigt.
2. Geben Sie im Textfeld **Suchen** einen beliebigen Text ein, nach dem Sie suchen möchten.
3. Wählen Sie in der Dropdown-Liste **In Spalte** die Spalte aus, die Sie durchsuchen möchte.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Suche**.

Die resultierende Liste zeigt nur die Elemente an, die Ihren Suchkriterien entsprechen.

Statusleiste

In der Statusleiste auf der Unterseite der Management Suite-Konsole wird Folgendes angezeigt:

- Anzahl der ausgewählten Elemente in einer Liste
- Aktueller Auftragsname und -status
- Name des gegenwärtig angemeldeten Benutzers
- Tage, bis der Core Server versuchen wird, den LANDesk Software-Lizenzserver zu kontaktieren.

Die Statusleiste wird stets angezeigt.

Starten der Management Suite-Konsole

So starten Sie die Management Suite-Konsole

1. Klicken Sie auf **Start** | **Programme** | **LANDesk | LANDesk Management Suite 8**.
2. Geben Sie einen gültigen Management Suite-Benutzernamen und ein -Kennwort eingeben.

   Halten Sie die üblichen Windows Richtlinien für die Remote-Anmeldung ein, wenn Sie eine Verbindung zu einem Remote-Core Server herstellen (d.h. wenn es sich bei diesem Core Server um einen lokalen Benutzer handelt, geben Sie lediglich den Benutzernamen ein; wenn es sich um einen Domänenbenutzer handelt, geben Sie den Domänennamen\Benutzernamen ein).

3. Wählen Sie den Core Server aus, zu dem Sie eine Verbindung herstellen möchten. Der Benutzer muss über die richtigen Berechtigungsnachweise für die Authentifizierung bei diesem Core Server verfügen.
4. Klicken Sie auf **OK**.

Die Management Suite-Konsole wird mit dem Layout geöffnet (Format, Position, geöffnete Werkzeugfenster etc), das vor dem Abmelden dieses Benutzers verwendet wurde.

Informationen über den Anmeldebildschirm der Management Suite

Verwenden Sie dieses Dialogfeld, um die Management Suite-Konsole zu starten und eine Verbindung zu einem Core Server herzustellen.

- **Benutzername:** Bezeichnet einen Benutzer der Management Suite. Es kann sich dabei um einen Administrator oder um einen anderen Management Suite-Benutzertyp mit eingeschränktem Zugriff handeln (siehe "Rollenbasierte Administration" weiter unten in diesem Kapitel). Dieser Benutzer muss ein Mitglied der LANDesk Management Suite-Gruppe auf dem Core Server sein. Wenn Sie eine Verbindung zu einem Remote-Core Server herstellen, geben Sie den Benutzernamen/die Domäne ein.
- **Kennwort:** Kennwort des Benutzers.

  Hinweis: Wenn ein Management Suite-Administrator das Kennwort eines anderen Benutzers ändert (d. h. ein zusätzlicher Konsolenbenutzer), wird das neue Kennwort erst nach dem Neustart der Konsole durch diesen Benutzer gültig. Der Benutzer gibt dann das neue Kennwort ein, um sich bei der Konsole anzumelden.

- **Core server:** Legt den Core Server fest, zu dem Sie eine Verbindung herstellen möchten. Diese Dropdownliste entspricht der Dropdownliste der Core Server, die in der Konsolensymbolleiste verfügbar ist.

Ändern der Core Server-Verbindung

Mit der Management Suite-Konsole können Sie die Inhalte jeder Datenbank anzeigen und verwalten, die mit einem Core Server verknüpft ist, zu dem Sie eine Verbindung im Netzwerk herstellen können. Dadurch können Sie Datenbanken für verschiedene Standorte, Organisationseinheiten oder logische interne Netzwerke erstellen.

Sie können nur jeweils mit einem Core Server verbunden sein.

So ändern Sie Core Server-Verbindungen

1. Wählen Sie einen Core Server aus der Dropdownliste **Core** in der Symbolleiste der Konsole. Sie können auch den Namen eines Core Servers in das Textfeld eingeben und die **Eingabetaste** drücken.

   Management Suite sucht nach dem Server im Netzwerk. Wenn er gefunden wurde, werden Sie aufgefordert, sich beim standardmäßigen Anmeldebildschirm der Management Suite anzumelden.

2. Geben Sie einen gültigen Management Suite-Benutzernamen und ein -Kennwort eingeben.

   Halten Sie die üblichen Windows NT-Richtlinien für die Remote-Anmeldung ein (d.h. wenn es sich bei diesem Core Server um einen lokalen Benutzer handelt, geben Sie lediglich den Namen ein; wenn es sich um einen Domänenbenutzer handelt, geben Sie den Domänennamen\Benutzernamen ein).

Sobald Sie mit dem Core Server verbunden sind, wird dessen Name automatisch zur Dropdownliste **Core** in der Symbolleiste hinzugefügt.

Verwenden der rollenbasierten Administration

Die rollenbasierte Administration ist eine leistungsstarke neue Funktion der LANDesk Management Suite 8. Administratoren (Benutzer mit LANDesk-Administratorrechten) können auf die rollenbasierten Administratorwerkzeuge zugreifen, indem Sie im Menü "Extras" oder in der Toolbox auf **Benutzer** klicken.

Durch die rollenbasierte Administration können Sie Benutzer zum Management Suite-System hinzufügen und diesen Benutzern spezielle administrative Rollen zuweisen, die auf ihren Rechten und ihrem Bereich basieren. *Rechte* bestimmen die Werkzeuge und Funktionen der Management Suite, die ein Benutzer anzeigen und verwenden kann (siehe "Erläuterungen zu Rechten" weiter unten in diesem Kapitel). *Bereich* bestimmt das Spektrum an Geräten, das ein Benutzer sehen und verwalten kann (siehe "Erstellen von Bereichen" weiter unten in diesem Kapitel).

Sie können Rollen für Benutzer erstellen, die auf den Verantwortungsbereichen, den Verwaltungstasks, die Sie ihnen einräumen möchten und den Geräten basieren, auf die sie zugreifen und die sie verwalten sollen. Der Zugriff auf Geräte kann geographisch eingeschränkt werden nach Ländern, Regionen, Bundesländern, Städten oder einzelnen Büros oder Abteilungen. Der Zugriff kann auch auf eine bestimmte Clientplattform, einen Prozessortyp oder andere Hard- und Softwareattribute von Geräten eingeschränkt werden. Bei der rollenbasierten Administration können Sie frei entscheiden, wie viele Rollen Sie erstellen möchten, welche Benutzer in diesen Rollen agieren und wie groß oder klein ihr Bereich des Gerätezugriffs sein soll.

Sie können z. B. einen oder mehrere Benutzer mit der Rolle des Softwareverteilungsverwalters und einen weiteren Benutzer einrichten, der für Fernsteuerungsvorgänge verantwortlich ist; einen Benutzer, der Berichte ausführt usw.

Administrative Beispielrollen

Die folgende Tabelle enthält einige der möglichen administrativen Rollen in Management Suite, die Sie vielleicht implementieren möchten, die allgemeinen Tasks, die Benutzer durchführen und die Rechte, die Benutzer benötigen, um diese Rolle effektiv erfüllen zu können.

Rolle	Tasks	Erforderliche Rechte
Administrator	Konfiguration von Core Servern, Installation von zusätzlichen Konsolen, Durchführung von Datenbank-Rollups, Verwaltung von Benutzern, Konfiguration von Alarmen, Integration von LANDesk-Systemverwalter usw. (natürlich können Administratoren mit vollen Rechten alle Verwaltungstasks durchführen).	LANDesk-Administrator (mit allen Rechten)

Inventarverwaltung	Erkennung von Geräten, Konfiguration von Clients, Ausführung des Inventarscanners, Erstellung und Verteilung von benutzerdefinierten Datenformularen, Aktivierung der Verfolgung des Inventarverlaufs etc.	Nicht verwaltete Geräteerkennung und Public Query Management
Helpdesk	Fernsteuerung von Clients, Chat, Dateiübertragung, Softwareausführung, Abschalten, Neustart, Anzeige von Agent und Status etc.	Fernsteuerung
Anwendungsverwalter	Verteilung von Softwarepaketen, Verwendung von Targeted Multicast und Peer Download, Aktivierung des Application Policy Management, Reparatur von Anwendungen etc.	Software Distribution
Migrationsverwalter	Erstellung von Abbildern, Verteilung von Betriebssystem-Abbildern, Migration von Benutzerprofilen, Erstellung und Verteilung von Profilmigrationspaketen, die von Benutzern initiiert wurden, Verteilung von PXE-Repräsentanten, Zuweisung von PXE-Warteschlangen, Konfiguration des PXE-Startmenüs, Erstellung von Startdisketten etc.	Betriebssystem-Verteilung
Berichtsverwalter	Ausführung von vordefinierten Berichten, Erstellung von benutzerdefinierten Berichten, Drucken von Berichten, Importieren und Exportieren von Berichten, Testen von Benutzerberichten etc.	Berichte (erforderlich für alle Berichte)
Softwarelizenüberwachungs-Verwalter	Konfiguration von Überwachungsanwendungen, Hinzufügen von Lizenzen, Erweitern und Reduzieren von Lizenzen, Prüfen von Berichten etc.	LANDesk-Administrator

Dies sind nur Beispielsrollen. Durch die Flexibilität der rollenbasierten Administration können Sie so viele benutzerdefinierte Rollen erstellen, wie Sie möchten. Sie können dieselben Rechte auch verschiedenen Benutzern zuweisen, aber ihren Zugriff auf einen begrenzten Satz von Geräten mit einem eingeschränkten Bereich beschränken. Sogar ein Administrator kann durch einen Bereich eingeschränkt werden, indem seine Administratoraufgaben auf eine bestimmte geographische Region oder einen bestimmten Typ von verwalteten Geräten eingeschränkt wird. Wie Sie am besten von der rollenbasierten Administration profitieren, hängt von Ihren Netzwerk- und Personalressourcen und von Ihren individuellen Bedürfnissen ab.

Um die rollenbasierte Administration zu implementieren und durchzuführen, erklären Sie einfach NT-Benutzer zu Management Suite-Benutzern oder Sie erstellen neue NT-Benutzer und fügen Sie hinzu und weisen ihnen die erforderlichen Rechte zu (zu Management Suite-Funktionen) sowie den Bereich (zu verwalteten Geräten). Führen Sie die folgenden Verfahren aus:

- Hinzufügen von Management Suite-Benutzern
- Erläuterungen zu Berechtigungen
- Erstellen von Bereichen
- Zuweisen von Rechten und Bereich an Benutzer

Hinzufügen von Management Suite-Benutzern

Management Suite-Benutzer sind Benutzer, die sich an der Management Suite-Konsole anmelden und bestimmte Tasks für bestimmte Geräte im Netzwerk durchführen können.

Management Suite-Benutzer werden nicht auf der Konsole erstellt. Benutzer werden dagegen in der Gruppe "Alle Benutzer" angezeigt (klicken Sie auf **Extras | Benutzer | Alle Benutzer**), nachdem Sie zur LANDesk Management Suite-Gruppe in der Windows NT-Benutzerumgebung auf dem Core Server hinzugefügt wurden. Die Gruppe "Alle Benutzer" zeigt alle Benutzer an, die gegenwärtig in der LANDesk Management Suite-Gruppe auf dem Core Server vorhanden sind.

Es gibt zwei Standardbenutzer in der Gruppe "Alle Benutzer":

- **Standardvorlagenbenutzer:** Dieser Benutzer ist im Grunde eine Vorlage von Benutzereigenschaften (Rechte und Bereich), die für die Konfiguration neuer Benutzer verwendet wird, wenn diese zur LANDesk Management Suite-Gruppe hinzugefügt werden. Wenn Sie also einen Benutzer zu dieser Gruppe in der Windows NT-Umgebung hinzufügen, erbt der Benutzer die Rechte und den Bereich, die aktuell in den Eigenschaften "Standardvorlagenbenutzer" definiert sind. Wenn für den "'Standardvorlagenbenutzer" alle Rechte ausgewählt und "Standardbereich: Alle Rechner" ausgewählt wurde, wird jeder neuer Benutzer der LANDesk Management Suite-Gruppe zur Gruppe "Alle Benutzer" hinzugefügt, mit den Zugriffsrechten auf alle Management Suite-Werkzeuge und alle Geräte.

  Sie können die Eigenschafteneinstellungen für "Standardvorlagenbenutzer" ändern, indem Sie ihn auswählen und auf **Benutzer bearbeiten** klicken. Wenn Sie z. B. eine große Zahl von Benutzern auf ein Mal hinzufügen möchten, von denen jedoch nicht alle Zugriff auf alle Werkzeuge oder Geräte haben sollen, ändern Sie zuerst die Einstellungen für den "Standardvorlagenbenutzer" und fügen dann die Benutzer zur LANDesk Management Suite-Gruppe hinzu (siehe folgende Schritte).

Der "Standardvorlagenbenutzer" kann nicht entfernt werden.

- **Standard-Administrator:** Dies ist der Benutzer, der am Server angemeldet war, als Management Suite installiert wurde.

Wenn Sie einen Benutzer zur LANDesk Management Suite-Gruppe in NT hinzufügen, wird der Benutzer automatisch in die Gruppe "Alle Benutzer" im Fenster "Benutzer" eingelesen und erbt dieselben Rechte und denselben Bereich wie der aktuelle "Standardvorlagenbenutzer". Es werden der Name, der Bereich und die Rechte des Benutzers angezeigt. Zusätzlich werden neue Benutzeruntergruppen, die nach der eindeutigen Anmelde-ID des Benutzers benannt werden, in den Gruppen "Benutzergeräte", "Benutzerabfragen", "Benutzerberichte" und "Benutzerskripts" erstellt (beachten Sie, dass NUR ein Administrator Benutzergruppen anzeigen kann).

Wenn Sie einen Benutzer aus der LANDesk Management Suite-Gruppe in der Windows-Benutzerumgebung entfernen, wird der Benutzer nicht mehr in der Gruppe "Alle Benutzer" angezeigt. Das Konto des Benutzers existiert weiterhin auf dem Server und kann jederzeit wieder zur LANDesk Management Suite-Gruppe hinzugefügt werden. Außerdem bleiben die Benutzeruntergruppen unter "Benutzergeräte", "Benutzerabfragen", "Benutzerberichte" und "Benutzerskripts" erhalten, sodass Sie den Benutzer ohne dessen Daten zu verlieren wiederherstellen können und Sie diese Daten in andere Benutzer kopieren können.

Um die Gruppe "Alle Benutzer" zu aktualisieren, damit neu hinzugefügte Benutzer angezeigt werden, klicken Sie mit der rechten Maustaste auf **Alle Benutzer** und auf **Aktualisieren**.

So kopieren Sie einen Benutzer in die LANDesk Management Suite-Gruppe

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppen | Gruppen** des Servers.
2. Klicken Sie mit der rechten Maustaste auf die Gruppe **LANDesk Management Suite** und auf **Hinzufügen**.
3. Wählen Sie einen (oder mehrere) Benutzer aus der Liste aus.
4. Klicken Sie auf **Hinzufügen** und **OK**.

Hinweis: Sie können auch einen Benutzer zur LANDesk Management Suite-Gruppe hinzufügen, indem Sie mit der rechten Maustaste auf das Benutzerkonto in der Benutzerliste klicken; klicken Sie auf **Eigenschaften | Mitglied von** und auf **Hinzufügen**, um die Gruppe auszuwählen und den Benutzer hinzuzufügen.

Wenn in NT noch keine Benutzerkonten vorhanden sind, müssen Sie sie zuerst auf dem Server erstellen.

So erstellen Sie ein neues Benutzerkonto

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppen | Benutzer** des Servers.
2. Klicken Sie mit der rechten Maustaste auf **Benutzer** und auf **Neuer Benutzer**.
3. Geben Sie im Dialogfeld "Neuer Benutzer" einen Namen und ein Kennwort ein.
4. Legen Sie die Kennworteinstellungen fest.

5. Klicken Sie auf **Erstellen**. Das Dialogfeld "Neuer Benutzer" bleibt geöffnet, sodass Sie zusätzliche Benutzer erstellen können.
6. Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.
7. Fügen Sie den Benutzer zur LANDesk Management Suite-Gruppe hinzu, damit er in der Gruppe "Alle Benutzer" in der Konsole angezeigt wird.

Sie können nun die Rechte und den Bereich der Management Suite-Benutzer zuweisen.

Erläuterungen zu Berechtigungen

Rechte verleihen den Zugriff auf bestimmte Management Suite-Werkzeuge und -Funktionen. Benutzer müssen über das erforderliche Recht (oder Rechte) verfügen, um entsprechende Aufgaben durchzuführen. Um Geräte im Bereich eines Benutzers fernzusteuern, muss ein Benutzer über das Fernsteuerungsrecht verfügen.

Wenn ein Recht einem Benutzer nicht zugewiesen wird, werden diesem Benutzer mit diesem Recht verknüpfte Werkzeuge nicht in der Management Suite-Konsole angezeigt. Wenn einem Benutzer z. B. das Softwareverteilungsrecht nicht verliehen wurde, werden die Werkzeuge Application Policy Management und Application Healing weder im Menü "Extras" noch in der Toolbox angezeigt.

Einzelheiten über die einzelnen Management Suite-Rechte und wie Rechte verwendet werden können, um administrative Rollen zu erstellen, finden Sie in den folgenden Beschreibungen.

Bereiche steuern den Zugriff auf Geräte
Wenn die Funktionen verwendet werden, die durch diese Rechte freigegeben sind, werden Benutzer stets durch ihren Bereich eingeschränkt (die Geräte, die sie sehen und beeinflussen können).

LANDesk-Administrator

Das LANDesk-Administratorrecht gewährt den vollen Zugriff auf alle Management Suite-Werkzeuge (die Verwendung dieses Werkzeugs ist jedoch immer noch auf die Geräte beschränkt, die zum Bereich des Administrators gehören).

Dies ist das Standardrecht für einen neu hinzugefügten Benutzer, sofern Sie die Einstellungen für den "Standardvorlagenbenutzer" nicht geändert haben.

Das LANDesk-Administratorrecht verleiht den Benutzern die folgenden Möglichkeiten:

- Anzeige und Zugriff auf die Benutzerwerkzeuge im Menü "Extras" und in der Toolbox
- Anzeige und Zugriff auf das Werkzeug "Softwarelizenzüberwachung" im Menü "Extras" und in der Toolbox
- Anzeige und Verwaltung der Gruppen "Benutzergeräte" in der Netzwerkansicht
- Anzeige und Verwaltung der Gruppen "Benutzerabfragen" in der Netzwerkansicht
- Anzeige und Verwaltung der Gruppen "Benutzerskripts" im Fenster "Skripts verwalten"

- Anzeige und Verwaltung der Gruppen "Benutzerberichte" im Fenster "Berichte"
- Anzeige und Konfiguration der Produktlizenzierung im Menü "Konfigurieren"
- Durchführung aller Management Suite-Tasks, die durch die anderen unten aufgeführten Rechte zulässig sind

---

Hinweis über Rechte und Werkzeuge
Das LANDesk-Administratorrecht ist exklusiv mit der Softwarelizenzüberwachung und den Werkzeugen "Benutzer" verknüpft. Wenn ein Benutzer nicht über das LANDesk-Administratorrecht verfügt, werden diese beiden Werkzeuge nicht in der Konsole angezeigt.

Alle Benutzer können, unabhängig von ihren zugewiesenen Rechten, diese universellen Funktionen sehen und verwenden: Inventaroptionen, Warnungsprotokoll und Alarmeinstellungen.

Alle anderen Werkzeuge in der Management Suite-Konsole sind mit einem entsprechenden Recht verknüpft (wie nachfolgend beschrieben).

Betriebssystem-Verteilung

Das Betriebssystem-Verteilungsrecht verleiht den Benutzern die folgenden Möglichkeiten:

- Anzeige und Zugriff auf das Werkzeug "Skripts verwalten" im Menü "Werkzeuge" und in der Toolbox
- Erstellen und Ausführen der Betriebssystem-Verteilung und der Profilmigrationsskripts
- Planen von Betriebssystem-Verteilung und von Profilmigrationstasks
- Konfigurieren von PXE-Repräsentanten mit dem PXE-Repräsentantenverteilungsskript
- Bezeichnen von PXE-Warteschlangen
- Konfigurieren des PXE-Startmenüs

Software Distribution

Das Softwareverteilungsrecht verleiht den Benutzern die folgenden Möglichkeiten:

- Anzeige und Zugriff auf das Werkzeug "Skripts verwalten" im Menü "Werkzeuge" und in der Toolbox
- Erstellen und Ausführen von Softwareverteilungsskripts
- Erstellen und Ausführen von Clientkonfigurationen
- Planen von anderen skriptbasierten Tasks (mit der Ausnahme von Betriebssystem-Verteilungs- und Profilmigrationsskripts)
- Erstellen und Verteilen von Benutzerdefinierten Datenformularen
- Anzeige und Zugriff auf das Werkzeug "Application Healing" im Menü "Extras" und in der Toolbox
- Erstellen und Verteilen von Anwendungsreparaturlisten (ARLs)
- Verteilen von Softwarepaketen über Anwendungsrichtlinien (APM)
- Anzeige von LDAP-Verzeichnisse

Berichte

Das Berichtsrecht verleiht den Benutzern die folgenden Möglichkeiten:

- Anzeige und Zugriff auf das Werkzeug "Berichte" im Menü "Extras" und in der Toolbox
- Ausführen von vordefinierten Berichten
- Erstellen und Ausführen von benutzerdefinierten Anlagenberichten

Fernsteuerung

Das Fernsteuerungsrecht verleiht den Benutzern die folgenden Möglichkeiten:

- Verwenden der Fernsteuerungsoptionen im Kontextmenü eines Geräts (anderenfalls sind sie abgeblendet)
- Fernsteuerung von Clients, auf denen der Fernsteuerungsagent geladen ist
- Reaktivieren, Abschalten und Neustart von Clients
- Chatten mit Clients
- Fernausführung von Clientprogrammen
- Übertragung von Dateien auf und von Clients

Nicht verwaltete Geräteerkennung

Das Recht zur "Nicht verwalteten Geräteerkennung" verleiht den Benutzern die folgenden Möglichkeiten:

- Anzeige und Zugriff auf das Werkzeug "Nicht verwaltete Geräteerkennung" im Menü "Extras" und in der Toolbox
- Erstellen von Scannerkonfigurationen und Ausführen von verschiedenen Arten des Erkennungsscans (CBA, NT-Domäne etc.)

Public Query Management

Das Recht "Public Query Management" verleiht den Benutzern die folgenden Möglichkeiten:

- Erstellen, Ändern, Kopieren, Löschen und Verschieben von Abfragen in der Gruppe "Öffentliche Abfragen" in der Netzwerkansicht. (Ohne dieses Recht können die Geräte in der Gruppe "Öffentliche Abfragen" nur angezeigt werden.)

Informationen zu den Patch Manager- und Inventarverwaltungsrechten

Das Patch Manager-Recht bezieht sich speziell auf das Patch Manager-Add-On, das möglicherweise in Ihrem Management Suite-Netzwerk installiert ist. Weitere Informationen finden Sie unter "Verwenden des Patch Manager-Add-On".

Die beiden Inventarverwaltungsrechte beziehen sich speziell auf das Add-On-Produkt zur Inventarverwaltung. Weitere Informationen finden Sie unter "Verwenden des Add-On-Produkts zur Inventarverwaltung".

Auch wenn die Add-On-Produkte nicht installiert sind, werden diese Rechte dennoch in der Liste angezeigt (aktiviert), wobei sie jedoch abgeblendet sind. Die Tools und Funktionen des jeweiligen Add-On-Produkts stehen folglich ebenfalls nicht zur Verfügung. Sobald ein Add-On-Produkt installiert ist, werden seine jeweiligen Rechte in dieser Liste aktiviert. Die aktivierten Rechte können ausgewählt werden, um den Zugriff auf die Funktionen des Add-On-Produkts freizugeben, oder die Auswahl kann aufgehoben werden, um den Zugriff zu verweigern.

Erstellen von Bereichen

Ein Bereich definiert die Geräte, die durch einen Management Suite-Benutzer angezeigt und verwaltet werden können.

Ein Bereich kann beliebig groß oder klein sein, alle verwaltete Geräte umfassen, die in eine Core-Datenbank gescannt wurden oder nur ein einziges Gerät. Diese Flexibilität, kombiniert mit dem modularen Werkzeugzugriff, macht aus der rollenbasierten Administration eine vielseitige Verwaltungsfunktion.

Standardbereiche

Die rollenbasierte Administration der Management Suite umfasst zwei Standardbereiche. Diese beiden vordefinierten Bereiche können hilfreich sein bei der Konfiguration der Benutzereigenschaften des Standardvorlagenbenutzers.

- **Standardmäßig keine Rechner:** Beinhaltet keine Geräte in der Datenbank.
- **Standardmäßig alle Rechner:** Beinhaltet alle verwalteten Geräte in der Datenbank.

Sie können die Standardbereiche weder bearbeiten noch entfernen.

Benutzerdefinierte Bereiche

Es gibt zwei Arten von benutzerdefinierten Bereichen, die Sie erstellen und Benutzern zuweisen können:

- **Abfragebasiert:** Beschränkt den Zugriff auf diejenigen Geräte, die einer benutzerdefinierten Abfragesuche entsprechen. Sie können eine vorhandene Abfrage auswählen oder neue Abfragen im Dialogfeld "Benutzern Geräte zuweisen" erstellen, um einen Bereich zu definieren. Beachten Sie, dass Sie auch Abfragen aus der Gruppe "Abfragen" der Netzwerkansicht direkt in die Gruppe "Bereiche" kopieren können. Weitere Informationen zum Erstellen von Abfragen finden Sie unter "Erstellen von Datenbankabfragen" in Kapitel 3.
- **Auf LDAP oder benutzerdefinierten Verzeichnissen basierend:** Steuert den Zugriff auf ausschließlich solche Geräte, die sich in einer Active Directory- oder einer NetWare eDirectory LDAP-kompatiblen Verzeichnisstruktur befinden bzw. in einem benutzerdefinierten Verzeichnispfad. Sie können Verzeichnispfade im Dialogfeld "Sichtbare Geräte auswählen" auswählen, um einen Bereich zu definieren.

Ein Management Suite-Benutzer kann nur mit jeweils einem Bereich verknüpft werden; ein Bereich kann jedoch mit mehreren Benutzern gleichzeitig verknüpft werden.

So erstellen Sie einen Bereich

1. Klicken Sie auf **Extras | Benutzer**.
2. Wählen Sie das Objekt **Bereiche** und klicken Sie auf die Symbolleistenschaltfläche **Neuer Bereich**. Alternativ dazu können Sie auch mit der rechten Maustaste auf **Bereiche** klicken und **Neuer Bereich** wählen.
3. Geben Sie im Dialogfeld **Benutzern Geräte zuweisen** einen Namen für den neuen Bereich ein.
4. Geben Sie die Art des Bereichs an, den Sie erstellen möchten - abfragebasiert oder verzeichnisbasiert - indem Sie auf eine der Schaltflächen klicken.
5. Wenn Sie "abfragebasiert" ausgewählt haben, klicken Sie auf **Neu**, definieren die Abfrage im Dialogfeld **Neue Bereichsabfrage** und klicken dann auf **OK**.
6. Wenn Sie verzeichnisbasiert ausgewählt haben, klicken Sie auf **Durchsuchen**, wählen die Speicherorte (LDAP und/oder benutzerdefiniertes Verzeichnis) aus der Liste "Sichtbare Geräte" und klicken auf **OK**.

   Klicken Sie auf das Plus- (+) oder das Minuszeichen (-), um Knoten in der Verzeichnisstruktur zu erweitern oder zu reduzieren. Sie können mehrere Speicherorte auswählen, indem Sie die Strg-Taste gedrückt halten und auf die gewünschten Speicherorte klicken. Alle Knoten unter einem ausgewählten übergeordneten Knoten sind im Bereich enthalten.

   LDAP-Verzeichnisspeicherorte werden durch den Active Directory- oder den eDirectory-Speicherort eines Clients bestimmt. Weitere Informationen finden Sie unter "Verwenden von Active Directory und eDirectory" weiter unten in diesem Kapitel.

   Benutzerdefinierte Verzeichnisspeicherorte werden bestimmt durch das Computerstandort-Attribut in der Inventardatenbank. Dieses Attribut wird während der Clientkonfiguration definiert. Weitere Informationen finden Sie unter "Ausführen des Client-Setup-Assistenten" in Kapitel 3.

7. Klicken Sie auf **OK**, um den Bereich zu speichern und das Dialogfeld zu schließen.

Informationen zum Dialogfeld "Benutzern Geräte zuweisen"

Mithilfe dieses Dialogfeldes erstellen oder bearbeiten Sie einen Bereich. Sie können auf dieses Dialogfeld zugreifen, indem Sie einen Bereich auswählen und auf die Symbolleistenschaltfläche **Bereich bearbeiten** klicken oder indem Sie mit der rechten Maustaste auf den Bereich und **Eigenschaften** klicken.

- **Bereichsname:** Identifiziert den Bereich.
- **Benutzer Erlaubnis erteilen zum Anzeigen der Geräte:**
  - **Auf Abfrage basierend:** Erstellt einen Bereich, dessen Gerätebereich durch eine benutzerdefinierte Abfrage bestimmt wird.

    - **Neu:** Öffnet das Dialogfeld "Neue Abfrage", in dem Sie eine Abfrage definieren und speichern können. Dasselbe Dialogfeld wird angezeigt, wenn Sie eine Datenbankabfrage in der Netzwerkansicht erstellen. (Beachten Sie, dass Sie auch Abfragen aus der Gruppe "Abfragen" der Netzwerkansicht direkt in die Gruppe "Bereiche" kopieren können.)
    - **Auf LDAP- oder benutzerdefiniertem Verzeichnis basierend:** Erstellt einen Bereich, dessen Gerätebereich durch den Gerätestandort bestimmt wird.
    - **Durchsuchen:** Öffnet das Fenster "Sichtbare Geräte", in dem Sie die Speicherorte auswählen können. Klicken Sie auf das Plus- (+) oder das Minuszeichen (-), um Knoten in der Verzeichnisstruktur zu erweitern oder zu reduzieren. Sie können mehrere Speicherorte auswählen, indem Sie die Strg-Taste gedrückt halten und auf die gewünschten Speicherorte klicken. Alle Knoten unter einem ausgewählten übergeordneten Knoten sind im Bereich enthalten.
- **Aktuelle Bereichsdefinition:** Zeigt die Abfrageanweisungen für einen abfragebasierten Bereich an und die Speicherortpfade für einen verzeichnisbasierten Bereich.
- **Abfrage bearbeiten:** Öffnet das Dialogfeld "Abfrage bearbeiten", in dem Sie Abfrageparameter und -Anweisungen ändern können.
- **OK:** Speichert den Bereich und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Verwenden von Active Directory und eDirectory

Die beiden folgenden Abschnitten enthalten Richtlinien für die Verwendung von Active Directory. und NetWare eDirectory-Speicherorten, um verzeichnisbasierte Bereiche zu definieren.

So werden Active Directory-Speicherorte unterstützt

Damit ein Active Directory-Speicherort als Computerstandort-Attribut in das Inventar eines Clients gescannt werden kann, muss der aktuell angemeldete Benutzer auf dem Client ein Domänenbenutzer sein.

Um ein Active Directory-basiertes Computerstandort-Attribut eines Client zu entfernen, muss der Administrator den Client von der Domäne trennen und ggf. das DNS-Suffix vom Computernamen des Clients entfernen.

So werden Netware eDirectory-Speicherorte unterstützt

Damit ein NetWare-Serverspeicherort (oder ein eDirectory auf einem Windows-Serverspeichert) als Computerstandort-Attribut im Inventar eines Clients berichtet wird, muss der Administrator dem öffentlichen Benutzer Rechte zum Durchsuchen des Containers übertragen, in dem sich der Client befindet.

Außerdem muss der NetWare-Servername (oder eDirectory auf einem Windows-Servernamen) zu einer IP-Adresse auflösbar sein.

Zuweisen von Rechten und Bereich an Benutzer

Nachdem Sie Management Suite-Benutzer hinzugefügt haben, über die Rechte und wie sie den Zugriff auf Funktionen und Werkzeuge steuern, Bescheid wissen und Gerätebereiche erstellt haben, um den Zugriff auf verwaltete Geräte zu gewähren oder einzuschränken, besteht der nächste Schritt bei der Einrichtung der rollenbasierten Administration in der Zuweisung der entsprechenden Rechte und eines Bereichs für jeden Benutzer.

Sie können die Rechte und den Bereich eines Benutzers jederzeit ändern.

Wenn Sie die Rechte oder den Bereich eines Benutzers ändern, werden diese Änderungen erst beim nächsten Anmelden dieses Benutzers am Core Server übernommen.

So weisen Sie Rechte und einen Bereich an Benutzer zu

1. Klicken Sie auf **Extras | Benutzer**.
2. Wählen Sie die Gruppe **Alle Benutzer** aus, um alle Benutzer anzuzeigen, die gegenwärtig Mitglied der LANDesk Management Suite-Gruppe in der Windows NT-Umgebung des Core Servers sind.

   Im rechten Fensterausschnitt wird eine Benutzerliste mit den Benutzernamen, dem aktuellen Bereich und zugewiesenen Rechten angezeigt (ein x-Zeichen gibt an, ob das Recht aktiviert oder aktiv ist).

   Sie können diese Liste aktualisieren, indem Sie mit der rechten Maustaste auf **Alle Benutzer** klicken und **Aktualisieren** wählen.

3. Klicken Sie einen Benutzer und die Symbolleistenschaltfläche **Benutzer bearbeiten** an.
4. Aktivieren oder deaktivieren Sie Rechte nach Bedarf im Dialogfeld "Benutzereigenschaften" (siehe Erläuterungen zu Rechten weiter oben in diesem Kapitel).
5. Wählen Sie einen Bereich aus der Liste "Verfügbare Bereiche" aus (siehe "Erstellen von Bereichen" weiter oben in diesem Kapitel).
6. Klicken Sie auf **OK**.

Die neuen Rechte und der Bereich werden neben dem Benutzernamen in der Liste angezeigt und wirksam, wenn der Benutzer das nächste Mal eine Verbindung zum Core Server herstellt.

Informationen zum Dialogfeld "Benutzereigenschaften"

Verwenden Sie dieses Dialogfeld, um die zugewiesenen Rechte und den zugewiesenen Bereich eines Benutzers anzuzeigen.

- **Zugewiesene Rechte:** Führt die Rechte auf, die dem Benutzer zugewiesen wurden (siehe "Erläuterungen zu Rechten" weiter oben in diesem Kapitel).
    - **LANDesk-Administrator**
    - **Betriebssystem-Verteilung**
    - **Software Distribution**
    - **Berichte**
    - **Fernsteuerung**
    - **Nicht verwaltete Geräteerkennung**
    - **Public Query Management**
- **Aktueller Bereich:** Gibt den aktuellen Bereich des Benutzers an.
- **Verfügbare Bereiche:** Führt alle Bereiche auf, die Sie mit dem Benutzer verknüpfen können.
- **Erstellen:** Öffnet das Dialogfeld "Benutzern Geräte zuweisen", in dem Sie eine neue Abfrage erstellen können - oder einen verzeichnisbasierten Bereich.
- **Bearbeiten:** Öffnet das Dialogfeld "Benutzern Geräte zuweisen", in dem Sie Änderungen am ausgewählten Bereich vornehmen können.
- **OK:** Speichert die Änderungen an den Benutzereigenschaften und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Konfigurieren der Agent-Erkennung

Die Management Suite verwendet die Agent-Erkennung, um verwaltete Clients zu suchen, auf denen CBA- oder Fernsteuerungsagenten installiert sind. Diese beiden Agenten ermöglichen die folgende Funktionalität:

- **CBA:** Der Common Base Agent aktiviert den PDS (Ping Discovery Service). Wenn der CBA auf einem Client installiert ist, können Sie Software Distributions und Clientsetupkonfigurationen planen.
- **Fernsteuerung:** Für den Fernzugriff und die Fernsteuerung eines Client.

Die Agent-Erkennung verwendet TCP/IP, um Agenten zu überprüfen, auf denen die Clients ausgeführt werden.

Um die CBA-Erkennung mit TCP/IP durchzuführen, verwendet die Management Suite IP-Adressen als Suchkriterien. Die Management Suite sucht nach CBA- und Fernsteuerungsagenten auf Clients innerhalb eines bestimmten Bereichs von IP-Adressen. Dieser Adressenbereich wird durch die von Ihnen angegebene IP-Netzwerkadresse vorgegeben.

Wenn Sie keine Subnetznetzwerkadressen bei der TCP/IP-Suche bezeichnen, führt die Management Suite die Erkennung nur in dem Netzwerksegment durch, in dem die Konsole resident ist, die die Erkennung initiiert. Wenn Sie z.B. vier Konsolen installiert haben, von denen jede auf einem anderen Netzwerksegment resident ist, müssten Sie vier Scans initiieren - einer von jeder der vier Konsolen aus.

Auf Netzwerksegmenten, auf denen die Konsolen nicht vorhanden sind, MÜSSEN Sie Subnetz-Netzwerkadressen verwenden, um auf die Daten dieses Netzwerksegments zuzugreifen.

Hinweis: Wenn Ihr Netzwerk mit einer oder mehreren Firewalls ausgestattet ist, kann die Management Suite keine CBA-Erkennung verwenden, um außerhalb Firewalls zu suchen, da Firewalls im Allgemeinen den Fluss des Paketdatenverkehrs zu deklarierten Ports begrenzen

---

So konfigurieren Sie Agent-Erkennungsoptionen

1. Klicken Sie auf **Konfigurieren | Agent-Erkennungsoptionen**.
2. Wählen Sie, ob die Agent-Erkennung den Agentenstatus nur für das ausgewählte Element in der Netzwerkansicht oder für alle sichtbaren Elemente in der Netzwerkansicht aktualisieren soll.
3. Legen Sie die Agentenstatus-Aktualisierungsrate fest.
4. Konfigurieren Sie, wie der Fernsteuerungsagent erkannt werden soll und räumen Sie der Adressenauflösungsmethode Priorität ein.
5. Legen Sie fest, wie lange die Agent-Erkennung versuchen soll, den Fernsteuerungsagenten auf dem Client vor dem Timeout zu erkennen.
6. Klicken Sie auf **OK**.

Informationen über das Dialogfeld "Agent-Erkennungsoptionen"

In diesem Dialogfeld können Sie die folgenden Erkennungsoptionen konfigurieren.

- **Agentenstatus erfassen:**
    - **Nur für ausgewählte Elemente:** Legt fest, dass der Agentenstatus eines Geräts aktualisiert wird, wenn das Gerät in der Netzwerkansicht ausgewählt wird. Diese Option führt zum geringsten Aufkommen von Netzwerkverkehr und ist die Standardeinstellung.
    - **Für alle in der Netzwerkansicht sichtbaren Elemente:** Legt fest, dass für alle sichtbaren Geräte in der Netzwerkansicht der Agentenstatus entsprechend der Aktualisierungsrate aktualisiert wird. Wenn neue Geräte sichtbar werden, wird ihr Agentenstatus (und der Zustand) aktualisiert.
- **Agentenstatus und Gerätezustand werden alle < > Minuten aktualisiert.** Gibt an, ob der Agentenstatus automatisch aktualisiert wird. Sie können die Aktualisierungsrate festlegen.
- **Ferngesteuerte Agent-Erkennung:**
    - **IP-Adresse:** Verwendet die Core-Datenbank, um die gespeicherte IP-Adresse des Computers abzurufen.
    - **Domain Name Service (DNS):** Löst den ID-Namen des Computers mit dem DNS-Server auf, wenn der Fernsteuerungsagent überprüft wird. Wenn Sie keinen DNS-Server haben, löschen Sie diese Option.
    - **Windows Internet Name Service (WINS):** Verwendet die NetBIOS-Namensauflösung.
    - **IP-Adressen aus Datenbank:** Verwendet die Core-Datenbank, um die gespeicherten IP-Adressen des Client zu ermitteln und testet jede einzelne. Computer können mehrere IP-Adressen in der Datenbank haben, wenn sie über mehrere Netzwerkkarten verfügen.
    - **Nach oben und unten verschieben:** Verschiebt die ausgewählte Methode in der Liste "Agent ermitteln mit". Die Methoden werden in der Reihenfolge getestet, in der sie in der Liste aufgeführt sind.
- **Timeout:** Legt den Timeoutwert fest, bevor die "Ferngesteuerte Agent-Erkennung" fehlschlägt für jede aktivierte Adressenauflösungsmethode.

Anzeigen von Geräteeigenschaften

In der Netzwerkansicht der Management Suite können Sie schnell Informationen über ein Gerät anzeigen, indem Sie das Gerät in der Geräteliste mit der rechten Maustaste anklicken und **Eigenschaften** auswählen.

Genauere Informationen über den Client sind in dessen Inventardaten enthalten. Sie können Inventardaten in den Netzwerkansichtsspalten anzeigen (die konfigurierbar sind) oder indem Sie den Client mit der rechten Maustaste anklicken und **Inventar** wählen, um das ganze Inventarfenster zu öffnen.

Informationen zum Dialogfeld "Geräteeigenschaften"

In diesem Dialogfeld können Sie nützliche Informationen über das ausgewählte Gerät anzeigen. Das Dialogfeld umfasst drei Registerkarten: Inventar, Gerät und Agenten. Klicken Sie auf die einzelnen Registerkarten, um die entsprechenden Informationen anzuzeigen.

Registerkarte "Inventar"

Die Registerkarte "Inventar" enthält eine Zusammenfassung der Inventardaten des Client. Eine detaillierte Beschreibung finden Sie unter "Anzeigen einer Inventarübersicht" in Kapitel 4.

Registerkarte "Gerät"

Die Registerkarte "Gerät" enthält grundlegende Informationen über einen Client, einschließlich dessen Standort und Identität im Netzwerk.

- **Gerät:**
  - **Name:** Der Name, der in der Core-Datenbank für dieses Gerät angezeigt wird.
  - **Typ:** Die Art des Geräts, wie Windows 2000 Server oder XP Workstation.
- **Netzwerk:**
  - **IP-Name:** Der IP-Name für das Gerät.
  - **IP-Adresse:** Die IP-Adresse, die dem Gerät zugewiesen wurde.
  - **WINS-Name:** Der WINS-Name, der dem Gerät zugewiesen wurde.

Registerkarte "Agenten"

Die Registerkarte "Agenten" enthält Informationen über den aktuellen Status von Agenten und die Fernsteuerungseinstellungen für den Client.

- **Common Base-Agent-Status:** Zeigt an, dass der Common Base Agent (CBA) auf dem Client geladen ist.
- **LANDesk Systemverwalterstatus:** Zeigt an, dass der LANDesk Systemverwalteragent auf dem Client geladen ist. Dieser Agent wird nur geladen, wenn Sie den LANDesk-Systemverwalter auf dem Core Server installiert haben und wenn der Systemverwalteragent auf diesen Client verteilt wurde. (Weitere Informationen finden Sie in Kapitel 2 "Konfigurieren von Clients".)
- **Fernsteuerungsagent-Status:** Zeigt an, ob der Fernsteuerungsagent auf dem Client geladen ist. Wenn dieser Agent nicht auf dem Client geladen ist, sind Fernsteuerungsvorgänge (wie Dateitransfer und Chat) nicht verfügbar.
- **Sicherheitstyp:** Zeigt das für den Client verwendete Fernsteuerungs-Sicherheitsmodell an. Zu den Optionen gehören: Lokale Vorlage, Windows NT-Sicherheit/lokale Vorlage und and Zertifikatbasierte/lokale Vorlage.
- **Zulassen:** Zeigt die Fernsteuerungsvorgänge an, die auf dem Client erlaubt sind. Diese Vorgänge wurden durch die Clientkonfiguration aktiviert.
- **Einstellungen:** Zeigt an, wie die Fernsteuerung reagiert, wenn Sie einen Interaktionsversuch mit dem Client unternehmen.
- **Sichtbare Indikatoren:** Legt fest, wie die Fernsteuerungsanzeige auf dem Client angezeigt wird.

Überwachen von Clients aus Gründen der Netzwerkkonnektivität

Mithilfe der Geräteüberwachung können Sie regelmäßig die Konnektivität der verwalteten Geräte überwachen.

Die Ping-Einstellungen sind spezifisch für das Gerät, das Sie ausgewählt haben. Wenn ein Gerät nicht mehr auf einen Ping reagiert (also offline ist), kann die Management Suite AMS-Alarmmeldungen generieren, um Sie zu benachrichtigen. Sie können auch Alarmmeldungen konfigurieren, die Sie darüber benachrichtigen, wenn Geräte wieder online sind.

Informationen zum Dialogfeld "Geräteüberwachung konfigurieren"

In diesem Dialogfeld können Sie die folgenden Geräteüberwachungsoptionen konfigurieren.

- **Diese Geräte überwachen:** Führt die gegenwärtig überwachten Geräte auf.
- **Hinzufügen:** Öffnet das Dialogfeld "Überwachte Geräte hinzufügen", in dem Sie nach verwalteten Geräten suchen und verwaltete Geräte aussuchen können, die Sie überwachen möchten.
- **Entfernen:** Entfernt das ausgewählte Gerät aus der Liste.
- **Ping-Frequenz: Steuert, wann und wie der Ping-Vorgang abläuft. Diese Einstellungen können auf jedes Gerät einzeln angewendet werden.**
  - **Ping alle:** Plant einen regelmäßigen Ping im festgelegten Minutenintervall.
  - **Täglich planen um:** Plant einen täglichen Ping zu einer festgelegten Zeit.
  - **Wdh:** Legt die Anzahl der Ping-Wiederholungen fest.
  - **Timeout:** Legt die Anzahl der Sekunden fest, bis das Timeout für die Ping-Wiederholungen eintritt.
- **Alarmeinstellungen:** Öffnet das Dialogfeld "AMS-Alarme konfigurieren", in dem Sie AMS-Alarmeinstellungen einrichten können, sodass Sie benachrichtigt werden, wann das Gerät offline oder online ist. Zu den Alarmeinstellungen gehört eine eigene Onlinehilfe, die Sie durch Klicken auf die Schaltfläche "Hilfe" öffnen können.
- **OK:** Speichert die Änderungen und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Konfigurieren von Geräteüberwachungswarnungen

Wenn Sie von der Geräteüberwachung benachrichtigt werden möchten, wenn verwaltete Geräte online oder offline gehen, müssen Sie zuerst die Alarmeinstellungen konfigurieren.

So konfigurieren Sie Geräteüberwachungs-Alarmeinstellungen

1. Klicken Sie im Dialogfeld "Geräteüberwachung konfigurieren" auf **Alarmeinstellungen**.

2. Erweitern Sie im Dialogfeld "Alarmkonfiguration" die Struktur **Geräteüberwachung**.
3. Wählen Sie den Alarm aus, die Sie konfigurieren möchten und klicken Sie auf **Konfigurieren**.
4. Wählen Sie eine Alarmaktion aus und klicken Sie auf **Weiter**.
5. Wählen Sie den Client aus, auf dem die Alarmaktion ausgeführt werden soll. Wählen Sie den Client, den Sie überwachen, nicht aus; wenn er offline geht, kann die Alarmaktion nicht verarbeitet werden.
6. Beenden Sie den Assistenten für die Alarmkonfiguration.

Hinweis: Wenn Sie Alarmeinstellungen konfigurieren, werden diese auf alle überwachten Clients angewendet.

Aktivieren des Core Server

LANDesk Software verwendet einen zentralen Lizenzserver, der Sie bei der Verwaltung der Produkt- und Knotenlizenzen Ihres Core Servers unterstützt. Um die LANDesk-Produkte verwenden zu können, müssen Sie von LANDesk einen Benutzernamen und ein Kennwort zur Aktivierung des Core Servers mit einem autorisierten Zertifikat anfordern. Die Aktivierung muss auf jedem Core Server durchgeführt werden, um die LANDesk-Produkte auf dem betreffenden Server verwenden zu können. Sie können jeden Core Server entweder automatisch über das Internet oder manuell per E-Mail aktivieren. Falls Sie die Hardwarekonfiguration des Core Servers entscheidend ändern, müssen Sie den Core Server u.U. reaktivieren.

Die Aktivierungskomponente des jeweiligen Core Servers generiert in regelmäßigen Abständen Daten in Bezug auf:

- Die genaue Anzahl von Knoten, die Sie verbrauchen.
- Die nicht persönliche verschlüsselte Hardwarekonfiguration.
- Die genauen LANDesk Softwareprogramme, die Sie verwenden ("Daten zur Knotenzahl")

Dies sind die einzigen Daten, die von der Aktivierung erfasst oder generiert werden. Der Code für den Hardwareschlüssel wird auf dem Core Server unter Verwendung nicht persönlicher Hardware-Konfigurationsfaktoren (beispielsweise die Größe der Festplatte, die Verarbeitungsgeschwindigkeit des Computers etc.) generiert. Der Code für den Hardwareschlüssel wird verschlüsselt an LANDesk gesendet und der private Schlüssel für die Verschlüsselung verbleibt ausschließlich auf dem Core Server. Der Code für den Hardwareschlüssel wird dann von LANDesk Software zur Erstellung eines Teils des autorisierten Zertifikats verwendet.

Aktivieren Sie den Core Server, nachdem Sie ihn installiert haben, mithilfe des Core Server-Aktivierungsprogramms (**Start | Programme | LANDesk | Core Server aktivieren**). Sie können den Core Server entweder mit einem LANDesk-Konto aktivieren, das mit den von Ihnen erworbenen Lizenzen verknüpft ist, oder mit einer 45 Tage gültigen Probelizenz. Die 45 Tage gültige Probelizenz deckt 100 Knoten ab. Es gibt zwei verschiedene Lizenztypen: Clientlizenz und Serverlizenz. Jedesmal, wenn Sie Management Suite-Agenten auf einem Serverbetriebssystem wie Windows 2000 Server oder Windows 2003 Server installieren, verbrauchen Sie eine Management Suite-Lizenz pro Server. Rollup-Core Server brauchen nicht aktiviert zu werden.

Sie können die 45-tägige Probelizenz jederzeit in eine Volllizenz konvertieren, indem Sie das Core Server-Aktivierungstool ausführen und den Benutzernamen und das Kennwort Ihrer LANDesk Software eingeben.

Jedesmal, wenn die Aktivierungssoftware auf einem Core Server die Daten zur Knotenzahl generiert, müssen Sie diese Daten entweder automatisch über das Internet oder manuell per E-Mail an LANDesk Software weiterleiten. Wenn Sie innerhalb einer Verzugsfrist von 30 Tagen - nach dem ersten Versuch, die Knotenzahl in Erfahrung zu bringen - keine Knotendaten bereitstellen, bleibt der Core Server so lange deaktiviert, bis LANDesk die entsprechenden Daten zur Knotenzahl von Ihnen erhalten hat. Sobald Sie die Daten zur Knotenzahl gesendet haben, erhalten Sie von LANDesk Software ein autorisiertes Zertifikat, mit dem sich der normale Betriebsmodus des Core Servers wieder aktivieren lässt.

Öffnen Sie nach der Aktivierung eines Core Servers in der Management Suite-Konsole das Dialogfeld **Konfigurieren | Produktlizenzierung**, um die Produkte und die Zahl der autorisierten Knoten anzuzeigen, die für das Konto, bei dem der Core Server authentiziert wird, erworben wurden. Sie können in diesem Dialogfeld auch überprüfen, an welchem Datum der Core Server die Daten zur Knotenzahl mit dem zentralen Lizenzserver abgleichen wird. Der Core Server schränkt Sie nicht auf die Anzahl der autorisierten Knoten ein, die Sie erworben haben. Informationen zu den von Ihnen verwendeten Lizenzen finden Sie auf der Lizenzierungs-Website der LANDesk Software unter www.landesk.com/contactus.

Informationen zum Core Server-Aktivierungsprogramm

Verwenden Sie das Core Server-Aktivierungsprogramm für folgende Aufgaben:

- Erste Aktivierung eines neuen Servers
- Aktualisierung eines vorhandenen Core Servers oder Konvertierung einer Probelizenz in eine Volllizenz
- Aktivierung eines neuen Servers mit einer 45 Tage gültigen Probelizenz

Starten Sie das Programm, indem Sie auf **Starte | Programme | LANDesk | Core Server aktivieren** klicken. Wenn Ihr Core Server nicht an das Internet angeschlossen ist, lesen Sie die Informationen unter "Manuelles Aktivieren eines Core oder Überprüfen der Daten zur Knotenzahl" weiter unten in diesem Abschnitt.

Jeder Core Server benötigt ein eindeutiges autorisiertes Zertifikat. Das Autorisierungszertifikat darf nicht von mehreren Core Servern gemeinsam benutzt werden; mehrere Core Server können jedoch Knotenzahlen beim selben LANDesk-Konto verifizieren lassen.

Der Core Server hinterlegt in regelmäßigen Abständen Verfizierungsdaten zur Knotenzahl in der Datei "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Diese Datei wird in regelmäßigen Abständen an den LANDesk Software-Lizenzserver gesendet. Die Datei wird im XML-Format erstellt und digital signiert und verschlüsselt. Jegliche Änderungen, die manuell an dieser Datei vorgenommen werden, machen ihren Inhalt und den nächsten Nutzungsbericht an den LANDesk Software-Lizenzserver ungültig.

Der Core kommuniziert mit dem LANDesk Software-Lizenzserver über HTTP. Wenn Sie einen Proxy-Server verwenden, klicken Sie auf die Registerkarte **Proxy** des Tools und geben Sie die erforderlichen Proxy-Informationen ein. Wenn Ihr Core über eine Internet-Verbindung verfügt, wird die Kommunikationsverbindung mit dem Lizenzserver automatisch, d.h. ohne Ihr Eingreifen, hergestellt.

Beachten Sie dass, dass das Core Server-Aktivierungstool keine DFÜ-Verbindung automatisch startet. Wenn Sie die DFÜ-Verbindung jedoch manuell starten und dann das Aktivierungstool ausführen, kann das Tool die Daten zur Nutzung auch über eine DFÜ-Verbindung weiterleiten.

Wenn Ihr Core Server nicht an das Internet angeschlossen ist, können Sie die Daten zur Knotenzahl auch manuell überprüfen und weiterleiten. Lesen Sie hierzu die Ausführungen weiter unten in diesem Abschnitt.

So aktivieren Sie einen Server mit einem LANDesk Software-Konto

Bevor Sie einen neuen Server mit einer Volllizenz aktivieren können, müssen Sie ein LANDesk Software-Konto eingerichtet haben, das Ihnen eine Lizenz für die von Ihnen erworbenen LANDesk Software-Produkte und Knoten erteilt hat. Sie benötigen die Kontoinformationen (Name der Kontaktperson und Kennwort), um Ihren Server zu aktivieren. Wenn Ihnen diese Informationen nicht vorliegen, wenden Sie sich an Ihren zuständigen Verkaufsvertreter bei LANDesk Software.

So aktivieren Sie einen Server

1. Klicken Sie auf **Start | Programme | LANDesk | Core Server aktivieren**.
2. Klicken Sie auf **Aktivieren Sie diesen Core Server mit Ihrem LANDesk-Kontaktnamen und Kennwort**.
3. Geben Sie den Namen der **Kontaktperson** und das **Kennwort** ein, den/das der Core verwenden soll.
4. Klicken Sie auf **Aktivieren**.

Aktivieren eines Servers mit einer Probelizenz

Die 45 Tage gültige Probelizenz aktiviert Ihren Server auf dem LANDesk Software-Lizenzserver. Nach Ablauf der 45-tägigen Testzeit können Sie sich nicht mehr beim Core Server anmelden und der Core Server nimmt keine Inventarscans mehr entgegen. Ihre in der Software oder Datenbank vorhandenen Daten gehen jedoch nicht verloren. Während oder nach Verwendung der 45-tägigen Probelizenz können Sie das Core Server-Aktivierungstool erneut ausführen und Ihre Probelizenz in eine Vollaktivierung konvertieren, die mit einem LANDesk Software-Konto arbeitet. Wenn die Probelizenz abgelaufen ist, wird mit der Konvertierung in eine Volllizenz der Core reaktiviert.

So aktivieren Sie eine 45-tägige Probelizenz

1. Klicken Sie auf **Start | Programme | LANDesk | Core Server aktivieren**.
2. Klicken Sie auf **Aktivieren Sie diesen Core für eine 45-tägige Testzeit**.
3. Klicken Sie auf **Auswerten**.

Aktualisieren eines vorhandenen Kontos

Die Aktualisierungsoption sendet Nutzungsdaten an LANDesk Software-Lizenzserver. Die Nutzungsdaten werden automatisch gesendet, wenn Ihr System über eine Internet-Verbindung verfügt. Es sollte sich daher im Allgemeinen für Sie nicht als notwendig erweisen, mit dieser Option Daten zur Verifizierung der Knotenzahl zu senden. Sie können diese Option auch verwenden, um das LANDesk Software-Konto zu ändern, dem der Core Server angehört. Zudem können Sie mit dieser Option einen Core Server von einer Probelizenz in eine Volllizenz konvertieren.

So aktualisieren Sie ein vorhandenes Kontos

1. Klicken Sie auf **Start | Programme | LANDesk | Core Server aktivieren**.
2. Klicken Sie auf **Dieser Core Server verwendet Ihren LANDesk-Kontaktnamen und Ihr Kennwort**.
3. Geben Sie den Namen der **Kontaktperson** und das **Kennwort** ein, den/das der Core verwenden soll. Wenn Sie einen Namen oder ein Kennwort eingeben, das sich von dem für die ursprüngliche Aktivierung des Core Servers verwendeten Namen oder Kennwort unterscheidet, wird der Core hiermit dem neuem Konto zugeordnet.
4. Klicken Sie auf **Aktualisieren**.

Manuelles Aktivieren eines Core oder Überprüfen der Daten zur Knotenzahl

Wenn der Core Server nicht an das Internet angeschlossen ist, kann das Core Server-Aktivierungstool keine Informationen bzgl. der Knotenzahl senden. In diesem Fall erhalten Sie eine Meldung, in der Sie aufgefordert werden, Verifizierungsdaten zur Aktivierung und zur Knotenzahl manuell per E-Mail zu senden. Die E-Mail-Aktivierung ist ein unkompliziertes und schnelles Verfahren. Wenn die Aufforderung zur manuellen Aktivierung auf dem Core angezeigt wird, oder wenn Sie das Core Server-Aktivierungstool verwenden und die manuelle Aktivierungsmeldung angezeigt wird, führen Sie folgende Schritte aus:

So aktivieren Sie einen Core manuell oder veranlassen Sie eine manuelle Verifizierung der Daten zur Knotenzahl

1. Wenn der Core Sie auffordert, die Daten zur Knotenzahl manuell zu verifizieren, erstellt er eine Datendatei mit dem Namen activate.xml im Ordner "\Program Files\LANDesk\ManagementSuite". Fügen Sie diese Datei einer E-Mail-Nachricht bei und senden Sie sie an licensing@landesk.com. Betreff und Nachrichtentext der Meldung können von Ihnen frei gewählt werden.
2. LANDesk Software verarbeitet beigefügte Datei und schickt eine Antwort an die E-Mail-Adresse, von der aus Sie die Nachricht gesendet hatten. Die LANDesk Software-Nachricht enthält Instruktionen und eine neue Autorisierungsdatei.
3. Öffnen Sie die beigefügte Autorisierungsdatei im Ordner "\Program Files\LANDesk\Authorization Files". Die Datei wird daraufhin sofort vom Core Server verarbeitet und ihr Aktivierungsstatus aktualisiert.

Wenn die manuelle Aktivierung misslingt oder der Core die beigefügte Aktivierungsdatei nicht verarbeiten kann, wird die von Ihnen kopierte Autorisierungsdatei unter Verwendung der Erweiterung ".rejected" umbenannt. Zusätzlich hierzu protokolliert das Aktivierungstool unter Angabe weiterer Details ein Ereignis im Anwendungsprotokoll der Windows-Ereignisanzeige.

Konfigurieren von Management Suite-Diensten

Sie können die folgenden Dienste für jeden der Core Server und Datenbanken konfigurieren:

- Auswählen eines Core Servers und einer Datenbank
- Inventar
- Scheduler
- Benutzerdefinierte Aufträge
- Multicast
- Betriebssystem-Verteilung

Legen Sie erst auf der Registerkarte "Allgemein" den Core Server und die Datenbank fest, für die Sie den Dienst konfigurieren möchten, bevor Sie einen Dienst konfigurieren.

Hinweis: Jegliche Änderungen an der Dienstkonfiguration, die Sie für einen Core Server und eine Datenbank vornehmen, wird erst übernommen, wenn Sie den Dienst auf dem Core Server neu starten.

Auswählen eines Core Servers und einer Datenbank mit den Einstellungen "Allgemein"

Auf der Registerkarte "Allgemein" können Sie einen Core Server und eine Datenbank auswählen und Authentifizierungsnachweise bereitstellen, sodass Sie Dienste für den Core Server konfigurieren können.

Informationen zum Dialogfeld "Management Suite-Dienste konfigurieren": Registerkarte "Allgemein"

Wählen Sie in diesem Dialogfeld den Core Server und die Datenbank aus, für die Sie einen bestimmten Dienst konfigurieren möchten. Wählen Sie dann die gewünschte Dienst-Registerkarte aus und legen Sie die Einstellungen für diesen Dienst fest.

- **Servername:** Zeigt den Namen des Core Servers an, mit dem Sie gegenwärtig verbunden sind.
- **Server:** Hier können Sie den Namen eines anderen Core Servers und dessen Datenbankverzeichnis eingeben.
- **Datenbank:** Hier können Sie den Namen der Core-Datenbank eingeben.
- **Benutzername:**Identifiziert einen Benutzer mit Berechtigungsnachweisen gegenüber der Core-Datenbank (während des Setup festgelegt).
- **Kennwort:** Identifiziert das Benutzerkennwort, das für den Zugriff auf die Core-Datenbank erforderlich ist (während des Setup festgelegt).
- **Dies ist eine Oracle-Datenbank:** Gibt an, dass die oben festgelegte Datenbank eine Oracle-Datenbank ist.
- **Einstellungen aktualisieren:** Stellt die vorhandenen Einstellungen wieder her, wenn Sie das Dialogfeld "Dienstkonfiguration" geöffnet haben.

Konfigurieren des Inventardienstes

Konfigurieren Sie auf der Registerkarte "Inventar" den Inventardienst für den Core Server und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben.

Informationen zum Dialogfeld "Management Suite-Dienste konfigurieren": Registerkarte "Inventar"

Definieren Sie mithilfe dieser Registerkarte die folgenden Inventaroptionen:

- **Servername:**Zeigt den Namen des Core Servers an, mit dem Sie gegenwärtig verbunden sind.
- **Statistik protokollieren:** P**rotokolliert Aktionen der Core-Datenbank und Statistiken.**
- **Server scanner unter:** Legt die Zeit für das Scannen des Core Servers fest.
- **Wartung durchführen unter:** Legt die **Zeit fest, um die Standardwartung der Core-Datenbank durchzuführen.**
- **Tage, die Inventarscans gespeichert bleiben::** Legt die **Zahl der Tage fest, bevor die Inventarscanaufzeichnung gelöscht wird.**
- **Anmeldedaten des primären Eigentümers:** Legt fest, wie oft der Inventarscanner Anmeldungen verfolgt, um den primären Eigentümer eines Geräts zu bestimmen. Der primäre Eigentümer ist der Benutzer, der sich innerhalb einer festgelegten Zahl von Anmeldungen am häufigsten angemeldet hat. Der Standardwert ist 5 und Mindest- bzw. Höchstwerte sind 1 bzw. 16. Wenn alle Anmeldungen eindeutig sind, wird der letzte Benutzer, der sich anmeldet, als primärer Eigentümer betrachtet. Ein Gerät kann nur jeweils mit einem primären Eigentümer verknüpft sein. Die Anmeldedaten des primären Eigentümers beinhalten den voll qualifizierten Namen des Benutzers entweder in ADS, NDS, den Domänennamen oder das lokale Namensformat (in dieser Reihenfolge) und das Datum der letzten Anmeldung.
- **Prüfeinstellungen:** Öffnet das Dialogfeld "Softwareprüfung", in dem Sie die Scanzeit der Clientsoftware und die Verlaufseinstellungen konfigurieren können.
- **ID duplizieren: Öffnet das Dialogfeld "Doppelte Gerätekennung", in dem Sie die Attribute auswählen können, die eindeutig Clients bezeichnen. Mit dieser Option können Sie vermeiden, dass doppelte Gerätekennungen in die Core-Datenbank gescannt werden (siehe "Konfigurieren des Vorgehens bei doppelten Gerätekennungen").**
- **Inventardienststatus: Zeigt an, ob der Dienst auf dem Core Server gestartet oder angehalten wurde.**
- **Start:** Startet den Dienst auf dem Core Server.
- **<b style="font-weight: bold;">Stopp:** Hält den Dienst auf dem Core Server an.

Informationen zum Dialogfeld "Softwareprüfung"

In diesem Dialogfeld können Sie die Häufigkeit von Softwarescans konfigurieren. Die Hardware eines Client wird jedes Mal gescannt, wenn der Inventarscanner auf dem Client ausgeführt wird; die Software eines Client wird jedoch nur in den Abständen gescannt, die Sie hier angeben.

- **Jede Anmeldung:** Scannt bei jeder Anmeldung des Benutzers die gesamte Software, die auf dem Client installiert.
- **Einmal alle (Tage):** Scannt die Clientsoftware automatisch nur in den festgelegten täglichen Abständen.
- **Verlauf speichern (Tage):** Legt fest, wie lange der Inventarverlauf des Client gespeichert bleibt.

Konfigurieren des Vorgehens bei doppelten Gerätekennungen

Da in Netzwerken häufig Abbilder verwendet werden, um Clients zu konfigurieren, besteht eine erhöhte Möglichkeit, dass es unter den Clients doppelte Gerätekennungen gibt. Sie können dieses Problem vermeiden, indem Sie andere Clientattribute verwenden, die in Kombination mit der Gerätekennung einen eindeutigen Bezeichner für Clients erstellen. Beispiele dieser anderen Attribute umfassen Gerätename, Domänenname, BIOS, Bus, Coprozessor usw.

Mit der Funktion "ID duplizieren" können Sie Clientattribute auswählen, die verwendet werden können, um den Client eindeutig zu bezeichnen. Sie legen die Art dieser Attribute fest und wie viele davon nicht vorhanden sein müssen, bevor der Client als ein Duplikat eines anderen Client deklariert wird. Wenn der Inventarscanner einen doppelten Client erkennt, schreibt er ein Ereignis in das Ereignisprotokoll der Anwendung, um die Gerätekennung des doppelten Client anzugeben.

So konfigurieren Sie die Behandlung von doppelten Kennungen

1. Klicken Sie auf **Konfigurieren | Dienste | Inventar | ID duplizieren**.
2. Wählen Sie Attribute aus der Liste der Attribute aus, die Sie verwenden möchten, um einen Client eindeutig zu bezeichnen und klicken Sie dann auf die Nach-rechts-Taste, um das Attribut zur Liste "Identitätsattribute" hinzuzufügen. Sie können beliebig viele Attribute hinzufügen.
3. Wählen Sie die Anzahl der Identitätsattribute (und der Hardwareattribute), bei denen keine Entsprechung vorliegen darf, damit der Client als Duplikat eines anderen Client gilt.
4. Wenn Sie möchten, dass doppelte Gerätekennungen zurückgewiesen werden, aktivieren Sie die Option **Doppelte Kennungen ablehnen**.

Informationen zum Dialogfeld "Doppelte Gerätekennung"

In diesem Dialogfeld können Sie das Vorgehen bei doppelten Gerätekennungen konfigurieren.

- **Attributsliste:** Führt alle Attribute auf, die Sie auswählen können, um eindeutig einen Client zu bezeichnen.
- **Identitätsattribute:** Zeigt die Attribute an, die Sie ausgewählt haben, um eindeutig einen Client zu bezeichnen.
- **Gerätekennungsauslöser duplizieren:**
  - **Identitätsattribute:** Bezeichnet die Anzahl der Attribute, bei denen keine Entsprechung vorliegen darf, damit der Client als Duplikat eines anderen Client gilt.

    - **Hardwareattribute:** Bezeichnet die Anzahl der Hardwareattribute, für die der Client keine Entsprechung vorlegen darf, damit dieser als Duplikat eines anderen Client ausgewiesen wird.
- **Doppelte Kennungen ablehnen:** Veranlasst den Inventarscanner, die Gerätekennung des doppelten Client aufzuzeichnen und jegliche folgenden Versuche, diese Gerätekennung zu scannen, abzulehnen. Der Inventarscanner generiert eine neue Gerätekennung.

Konfigurieren des Scheduler-Dienstes

Auf der Registerkarte "Scheduler" konfigurieren Sie den Scheduler-Dienst (**Extras | Geplante Tasks**) für den Core Server und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben.

Sie müssen über die entsprechenden Rechte verfügen, um diese Tasks auszuführen, einschließlich voller Administratorprivilegien für die Windows NT/2000-Clients im Netzwerk, die der Erlaubnis bedürfen, Paketverteilungen von der LANDesk Management Suite zu empfangen. Sie können mehrere auf den Clients zu verwendende Berechtigungsnachweise für die Anmeldung angeben, indem Sie auf **Anmeldedaten ändern** klicken.

Eine zusätzliche Einstellung, die Sie manuell konfigurieren können, ist die Aktualisierungsrate der geplanten Task. Standardmäßig prüft der Fensterausschnitt "Geplante Tasks" die Core-Datenbank, um zu bestimmen, ob sichtbare Elemente aktualisiert wurden. Wenn Sie die Aktualisierungsrate ändern möchten, navigieren Sie in der Registrierung zu diesem Schlüssel:

`HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\LDWM\TaskLog`

Fügen Sie einen neuen DWORD-Wert hinzu, nennen Sie ihn "RefreshRate", und geben Sie die Anzahl der Sekunden für die Aktualisierungsrate ein. Sie müssen den Intel Scheduler neu starten, damit der neue Schlüssel übernommen wird.

Informationen zum Dialogfeld "Management Suite-Dienste konfigurieren": Registerkarte "Scheduler"

Mithilfe dieser Registerkarte können Sie den Namen des Core Servers und der Datenbank anzeigen, die Sie zuvor ausgewählt haben und die folgenden Optionen der "Geplanten Tasks" festlegen:

- **Benutzername:** Der Benutzername, unter dem der Dienst "Geplante Tasks" ausgeführt wird. Er kann durch Klicken auf die Schaltfläche **Anmeldedaten ändern** geändert werden.
- **Anzahl Sek. zw. Wiederholungsversuchen:** Wenn eine geplante Task mit mehreren Wiederholungen konfiguriert ist, steuert diese Einstellung die Anzahl der Sekunden, die vor einer Wiederholung der Task vergehen müssen.
- **Anzahl Sek. für Reaktivierungsversuche:** Wenn eine geplante Task mit Wake On LAN konfiguriert ist, steuert diese Einstellung die Anzahl der Sekunden, die vor einer Reaktivierung der Task vergehen müssen.
- **Intervall zwischen Abfrageevaluierungen:** Eine Zahl, die die Zeitspanne zwischen Abfrageauswertungen angibt sowie eine Maßeinheit für die Zahl (Minuten, Stunden, Tage oder Wochen).

- **Wake on LAN-Einstellungen:**Der IP-Port, der von dem Wake On LAN-Paket verwendet wird, das von den geplanten Tasks zum Reaktivieren von Clients konfiguriert wurde.
- **Status des Planungsdiensts:** Zeigt an, ob der Dienst auf dem Core Server gestartet oder angehalten wurde.
- **Start:** Startet den Dienst auf dem Core Server.
- <b style="font-weight: bold;">Stopp: Hält den Dienst auf dem Core Server an.

Informationen zum Dialogfeld "Management Suite-Dienset konfigurieren": Dialogfeld "Anmeldedaten ändern"

Verwenden Sie das Dialogfeld "Anmeldedaten ändern" (auf der Registerkarte "Configure Services Scheduler" auf **Anmeldedaten ändern** klicken), um die Standard-Scheduler-Anmeldung zu ändern. Sie können zudem auch alternative Berechtigungsnachweise konfigurieren, die vom Scheduler-Dienst eingegeben werden sollten, wenn dieser einen Task auf nicht verwalteten Clients ausführen muss.

Um Management Suite-Agenten auf nicht verwalteten Clients zu installieren, muss der Scheduler-Dienst in der Lage sein, mit einem administrativen Konto Verbindungen zu Clients herzustellen. LocalSystem ist das vom Scheduler-Dienst verwendete Standardkonto. Die LocalSystem-Berechtigungsnachweise funktionieren im Allgemeinen für Clients, die sich in derselben Windows-Domäne befinden wie der Core Server.

Wenn Sie die Berechtigungsnachweise für die Anmeldung des Scheduler-Dienstes ändern möchten, können Sie ein anderes Domänenebene-Verwaltungskonto zur Verwendung auf Clients angeben. Wenn Sie Clients über mehrere Domänen hinweg verwalten, können Sie zusätzliche Berechtigungsnachweise hinzufügen, die der Scheduler-Dienst versuchsweise verwenden kann. Wenn Sie anstatt des LocalSystem-Kontos ein anderes Konto für den Scheduler-Dienst verwenden möchten, oder wenn Sie alternative Berechtigungsnachweise anbieten möchten, müssen Sie eine primäre Scheduler-Dienst-Anmeldung angeben, die über Core Server-Verwaltungsrechte verfügt. Alternative Berechtigungsnachweise machen keine Core Server-Verwaltungsrechte zur Bedingung, sie müssen jedoch Verwaltungsrechte auf Clients besitzen.

Bei Verwendung alternativer Berechtigungsnachweise für Windows 9x-Clients müssen Sie im Dialogfeld "Alternativen-Authentifizierung" den Benutzernamen "Administrator" angeben. Dasselbe Konto muss auf dem Server existieren, bei dem der Client seine Authentifizierung durchführt. Auf jedem Windows 9x-Client muss zudem auf der Registerkarte **Zugriffssteuerung** des Dialogfelds **Netzwerkeigenschaften** die Option **Zugriff auf Benutzerebene** ausgewählt sein. Dort können Sie den Namen des Windows NT/2000/2003-Servers eingeben, bei dem der Client seine Authentifizierung durchführt.

Der Scheduler-Dienst versucht zunächst, sich mit den Standard-Berechtigungsnachweise anzumelden. Wenn dies nicht gelingt, wiederholt er den Vorgang so lange mit jedem einzelnen Berechtegigungsnachweis, den Sie in der Liste **Alternativen-Authentifizierung** angegeben haben, bis keine Berechtigungsnachweise mehr vorhanden sind, mit denen er versuchen könnte, sich anzumelden. Von Ihnen angegebene Berechtigungsnachweise werden verschlüsselt und in der Registrierung des Core Servers gespeichert.

Sie können die folgenden Optionen für die Standard-Scheduler-Berechtigungsnachweise festlegen:

- **Benutzername:** Geben Sie den Standarddomänennamen\Standardbenutzernamen oder den Benutzernamen ein, den der Scheduler verwenden soll.
- **Kennwort:** Geben Sie das Kennwort für die von Ihnen festgelegten Berechtigungsnachweise ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein, um es zu bestätigen.

Sie können die folgenden Optionen für zusätzliche Scheduler-Berechtigungsnachweise festlegen:

- **Hinzufügen:** Klicken Sie, um den Benutzernahmen und das Kennwort hinzuzufügen, das Sie in der Liste "Alternativen-Authentifizierung" angegeben haben.
- **Entfernen:** Klicken Sie, um den ausgewählten Berechtigungsnachweis aus der Liste zu entfernen.
- **Ändern:** Klicken Sie, um die ausgewählten Berechtigungsnachweise zu ändern.

Geben Sie beim Hinzufügen alternativer Berechtigungsnachweise Folgendes an:

- **Benutzername:** Geben Sie den Benutzernamen ein, den der Scheduler verwenden soll.
- **Domäne:** Geben Sie die Domäne für den von Ihnen angegebenen Benutzernamen ein.
- **Kennwort:** Geben Sie das Kennwort für die von Ihnen festgelegten Berechtigungsnachweise ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein, um es zu bestätigen.

Konfigurieren des benutzerdefinierten Auftragsdienstes

Konfigurieren Sie auf der Registerkarte "Benutzerdefinierte Aufträge" die "Benutzerdefinierte Jobverarbeitung" für den Core Server und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben. Beispiele für benutzerdefinierte Aufträge schließen Inventarscans, Clientimplementierungen oder Softwareverteilungen ein.

Wenn Sie die TCP-Fernausführung als Fernausführungsprotokoll deaktivieren, verwendet "Benutzerdefinierte Aufträge" standardmäßig das CBA-Protokoll, unabhängig davon, ob es deaktiviert ist oder nicht. Wenn sowohl die TCP-Fernausführung als auch CBA aktiviert sind, versucht "Benutzerdefinierte Aufträge" zuerst, die TCP-Fernausführung zu verwenden. Wenn diese nicht vorhanden ist, wird die CBA-Fernausführung verwendet.

Auf der Registerkarte "Benutzerdefinierte Aufträge" können Sie Optionen für die Clienterkennung auswählen Damit die benutzerdefinierte Auftragsverarbeitung einen Auftrag bearbeiten kann, muss sie die aktuelle IP-Adresse des Clients ausfindig machen. Mit dieser Registerkarte können Sie festlegen, wie der Dienst mit den Clients Kontakt aufnimmt.

Informationen zum Dialogfeld "Management Suite-Dienste konfigurieren": Registerkarte "Benutzerdefinierte Aufträge"

Definieren Sie mithilfe dieser Registerkarte die folgenden Optionen für "Benutzerdefinierte Aufträge":

Fernausführungsoptionen:

- **Deaktiviert TCP-Ausführung:**Deaktiviert TCP als Fernausführungsprotokoll und verwendet standardmäßig das CBA-Protokoll.
- **CBA-Ausführung / Dateitransfer deaktivieren:** Deaktiviert CBA als Fernausführungsprotokoll. Wenn CBA deaktiviert ist und das TCP-Fernausführungsprotokoll nicht auf dem Client gefunden wird, schlägt die Fernausführung fehl.
- **Timeout f. Fernausführung aktivieren:** Aktiviert ein Fernausführungstimeout und legt die Zahl der Sekunden fest, nach der das Timeout eintritt. Fernausführungstimeouts werden ausgelöst, wenn der Client Heartbeat-Signale aussendet, der Auftrag auf dem Client jedoch hängt oder sich in einer Schleife befindet. Diese Einstellung wird auf beide Protokolle angewendet (TCP oder CBA). Dieser Wert kann zwischen 300 Sekunden (5 Minuten) und 86400 Sekunden liegen (1 Tag).
- **Client-Timeout aktivieren:**Aktiviert ein Client-Timeout und legt fest, nach wievielen Sekunden das Timeout eintritt. Standardmäßig sendet die TCP-Fernausführung ein Heartbeat-Signal vom Client an den Server in Intervallen von 45 Sekunden, bis die Fernausführung abgeschlossen oder ein Timeout eingetreten ist. Clienttimeouts werden ausgelöst, wenn der Client kein Heartbeat-Signal an den Server sendet.
- **Fernausführungsport (Standard 12174):** Der Port, über den die TCP-Fernausführung stattfindet. Wenn dieser Port geändert wird, muss er auch in der Clientkonfiguration geändert werden.

Verteilungsoptionen:

- **Verteilen an <nn> Clients gleichzeitig:** Die maximale Anzahl an Clients, auf die benutzerdefinierte Aufträge gleichzeitig verteilt werden.

Erkennungsoptionen:

- **UDP:** Wenn Sie UDP auswählen, wird ein Common Base Agent 8 (CBA)-Ping über UDP verwendet. Die meisten Management Suite-Clientkomponenten setzen CBA voraus. Aus diesem Grund sollte auf Ihren verwalteten Clients CBA installiert sein. Dies ist die schnellste Erkennungsmethode und gleichzeitig der Standard. Mit UDP können Sie auch die **Wiederholungen** und das **Timeout** für den UDP-Ping auswählen.

- **TCP:** Wenn Sie TCP auswählen, wird eine HTTP-Verbindung mit dem Client auf Port 9595 benutzt. Diese Erkennungsmethode hat den Vorteil, dass sie über eine Firewall hinweg einsatzfähig ist, wenn Sie Port 9595 öffnen; die Methode unterliegt jedoch HTTP-Verbindungs-Timeouts, wenn keine Clients vorhanden sind. Diese Timeouts können 20 Sekunden oder länger beanspruchen. Wenn eine große Zahl von Zielclients nicht auf die TCP-Verbindung reagiert, wird es einige Zeit dauern, bis Ihr Auftrag gestartet werden kann.
- **Beide:** Wenn Sie "Beide" auswählen, versucht der Dienst die Erkennung erst mit UDP, dann mit TCP und zuletzt mit DNS/WINS (sofern ausgewählt) durchzuführen.
- **Subnetz-Broadcast deaktivieren:** Wenn Sie diese Option auswählen, wird die Erkennung über ein Subnetz-Broadcast deaktiviert.
- **DNS/WINS:** Wenn diese Option ausgewählt ist, deaktiviert sie einen Name Service Lookup für jeden Client, wenn die ausgewählte TCP/UDP-Erkennungsmethode scheitert.

Konfigurieren des Multicast-Dienstes

Konfigurieren Sie auf der Registerkarte "Multicast" die Erkennungsoptionen für Multicast-Domänenrepräsentanten für den Core Server und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben.

Informationen zum Dialogfeld "Management Suite-Dienste konfigurieren": Registerkarte "Multicast"

Definieren Sie mithilfe dieser Registerkarte die folgenden Multicast-Optionen:

- **Multicast-Domänenrepräsentanten:** Verwendet die Liste mit den Multicast-Domänenrepräsentanten, die in der Gruppe "Konfiguration > Multicast-Domänenrepräsentanten" der Netzwerkansicht gespeichert ist.
- **Cachedatei verwenden:** Fragt jede Multicast-Domäne ab, um herauszufinden, wer die Datei bereits besitzt; in diesem Fall wird die Datei nicht auf einen Repräsentanten heruntergeladen.
- **Cachdatei vor bevorzugtem Domänenrepräsentanten verwenden:** Ändert die Reihenfolge der Erkennung, sodass "Cachedatei verwenden" die erste getestete Option ist.
- **Broadcast verwenden:** Sendet einen Subnetz-Broadcast, um Clients in diesem Subnetz zu finden, die Multicast-Domänenrepräsentanten sein könnten.
- **Verwerfungszeitraum (Tage) protokollieren:** Legt die Anzahl der Tage fest, die Einträge im Protokoll bis zum Löschen erhalten bleiben.

Konfigurieren des Betriebssystem-Verteilungsdienstes

Auf der Registerkarte "Betriebssystem-Verteilung" können Sie PXE-Repräsentanten als PXE-Warteschlangen deklarieren und grundlegende PXE-Startoptionen für den Core Server und die Datenbank konfigurieren, die Sie auf der Registerkarte "Allgemein" ausgewählt haben.

PXE-Warteschlangen sind eine Methode der Verteilung von Betriebssystemabbildern auf PXE-aktivierte Clients. Sie erklären vorhandene PXE-Repräsentanten (in der Gruppe "Konfiguration" in der Netzwerkansicht) als PXE-Warteschlangen. Weitere Informationen finden Sie unter "PXE-basierte Verteilung" in Kapitel 9.

Wählen Sie die PXE-Repräsentanten aus, und verschieben Sie sie von der Liste "Verfügbare Proxies" in die Liste "Haltewarteschlangen-Proxies".

Informationen zum Dialogfeld "Management Suite-Dienste konfigurieren": Registerkarte "Betriebssystem-Verteilung"

Verwenden Sie diese Registerkarte, um PXE-Haltewarteschlangen-Proxies (Repräsentanten) zuzuweisen und die PXE-Startoptionen zu definieren.

- **Verfügbare Proxies:** Führt alle im Netzwerk verfügbaren PXE-Proxies auf, bezeichnet durch ihren Clientnamen. Diese Liste wird generiert, wenn der Inventarscanner PXE-Software (PXE- und MTFTP-Protokolle) erkennt, die auf dem Client ausgeführt wird.
- **Haltewarteschlangen-Proxies:** Führt die PXE-Proxies auf, die von der Liste "Verfügbare Proxies" verschoben wurden und den Proxy als PXE-Haltewarteschlange deklarieren. PXE-aktivierte Clients auf demselben Subnetz wie der PXE-Haltwarteschlangen-Proxy werden automatisch zur Gruppe der PXE-Haltewarteschlangen in der Netzwerkansicht der Konsole hinzugefügt, wenn für sie ein PXE-Start durchgeführt wird. Anschließend kann für die Clients ein Abbildbereitstellungsauftrag geplant werden.
- **Zurücksetzen:** Erzwingt, dass alle PXE-fähigen Clients, die sich im selben Subnetz wie der ausgewählte PXE-Repräsentant befinden, wieder in die PXE-Haltewarteschlangengruppe in der Netzwerkansicht der Konsole eingefügt werden. Für diese Clients kann dann ein Abbildverarbeitungsauftrag geplant werden. (Die Schaltfläche "Zurücksetzen" wird aktiviert, wenn Sie einen PXE-Proxy in der Liste "Haltewarteschlangen-Proxies" auswählen.
- **PXE-Startoptionen:**Bestimmt das Verhalten der Eingabeaufforderung für den PXE-start, wenn Clients einen PXE-Startversuch unternehmen.

  > **Hinweis:** Änderungen, die Sie hier an den PXE-Startoptionen vornehmen, wirken sich erst dann auf die PXE-Repräsentanten aus, wenn Sie das PXE-Repräsentantenverteilungsskript auf diesem Repräsentanten ausführen.

- **Timeout:** Gibt an, wie lange die Start-Eingabeaufforderung bis zum Timeout angezeigt und wann der Standardstartvorgang wieder aufgenommen wird. Es können maximal 60 Sekunden eingegeben werden.
- **Meldung:** Legt die PXE-Start-Eingabeaufforderung fest, die auf dem Client angezeigt wird. Sie können jede beliebige Meldung in das Textfeld eingeben, bis zu einer maximalen Länge von 75 Zeichen.

Kapitel 2: Konfigurieren der Clients

Damit die Clients voll einsatzfähig sind, müssen die Management Suite-Agenten installiert sein. In diesem Kapitel erfahren Sie mehr über:

- Client-Agent-Sicherheit und vertrauenswürdige Zertifikate
- Erstellen einer Clientsetup-Konfiguration
- Übermitteln einer Clientkonfiguration an einen bereits vorhandenen Agenten
- Planen von Tasks
- Verwenden von "Nicht verwaltete Geräteerkennung"
- Ausführen des Client-Setup-Assistenten
    - Verteilung der Fernsteuerung
    - Verteilen des Inventars
    - Verteilen von Application Healing
    - Verteilen von Application Policy Management
    - Verteilen der Bandbreitenerkennung
    - Verteilen benutzerdefinierter Datenformulare
    - Aktivieren von Migrationstasks
    - Verteilen von Enhanced Software Distribution
    - Verteilen von Local Scheduler
    - Verteilen der Softwarelizenzüberwachung
    - Verteilen von Targeted Multicasting
    - Verteilen des Agenten "Taskfertigstellen"

Mithilfe des Client-Setup-Assistenten können Sie neue Setup-Konfigurationen für die Windows-Clients erstellen. Die neuen Clientkonfigurationen, die Sie mit dem Assistenten erstellen, können anschließend über das Konsolenfenster "Geplante Tasks" an Clients übermittelt werden.

Um eine neue Konfiguration zu erstellen und an Clients zu übermitteln, muss der CBA oder der Fernsteuerungsagent installiert sein. Für die Clients muss die Verwaltung aktiviert sein. Weitere Informationen finden Sie im *Installations- und Verteilungshandbuch*.

Erstellen von Client-Konfigurationen für Windows NT-/2000-/2003-/XP-Computer, für die die Verwaltung nicht aktiviert ist
Wenn Sie über Windows NT-/2000-/2003-/XP-Clients verfügen, die Teil einer Windows NT-/2000-/2003-/XP-Domäne sind, können Sie an diese Clients eine Konfiguration auch dann übermitteln, wenn der CBA und der Fernsteuerungsassistent nicht installiert sind. Weitere Informationen finden Sie im *Installations- und Verteilungshandbuch*.

Client-Agent-Sicherheit und vertrauenswürdige Zertifikate

Bei der Management Suite 8 wurde die zertifikatbasierte Authentifizierung vereinfacht. Clientagenten werden immer noch bei autorisierten Core Servern authentifiziert, um den nicht autorisierten Zugriff von Cores auf Clients zu verhindern. Management Suite 8 erfordert keine separate Zertifikatsautorität, um Zertifikate für den Core, die Konsole und jeden Client zu verwalten. Dagegen hat jeder Core Server ein eindeutiges Zertifikat und einen privaten Schlüssel, den Management Suite-Setup erstellt, wenn Sie zum ersten Mal den Core oder den Rollup-Core Server installieren.

Dies sind die privaten Schlüssel und die Zertifikatdateien:

- **<Schlüsselname>.key:**Die .KEY-Datei ist der private Schlüssel für den Core Server; sie ist nur auf dem Core Server resident. Wenn dieser Schlüssel gefährdet ist, sind Core Server und die Clientkommunikation nicht mehr sicher. Achten Sie auf die Sicherheit dieses Schlüssels. Senden Sie ihn beispielsweise nicht per E-Mail.
- **<Schlüsselname>.crt:**Die .CRT-Datei enthält den öffentlichen Schlüssel für den Core Server. Die .CRT-Datei ist eine anzeigefreundliche Version des öffentlichen Schlüssels, die Sie anzeigen können, um weitere Informationen über den Schlüssel zu erhalten.
- **<hash>.0:**Die .0-Datei ist eine vertrauenswürdige Zertifikatsdatei, deren Inhalt mit der .CRT-Datei identisch ist. Sie wird jedoch so benannt, dass der Computer die Zertifikatdatei in einem Verzeichnis schnell findet, das viele verschiedene Zertifikate enthält. Der Name entspricht einem Hash (Prüfsumme) der Subjektinformationen der Zertifikate. Um den Hash-Dateinamen eines bestimmten Zertifikats zu bestimmen, zeigen Sie die <Schlüsselname>.CRT-Datei an. Die Datei enthält einen .INI-Dateiabschnitt [LDMS]. Das Hash=Wert-Paar gibt den <Hash>-Wert an.

Alternativ kann der Hash auch bestimmt werden mithilfe der Anwendung openssl, die im Verzeichnis \Programme\LANDesk\Shared Files\Keys gespeichert ist. Sie zeigt unter Verwendung der folgenden Befehlszeile den assoziierten Hash mit einem Zertifikat an:

```
openssl.exe x509 -in <Schlüsselname>.crt -hash -noout
```

Alle Schlüssel sind auf dem Core Server gespeichert unter \Programme\LANDesk\Shared Files\Keys. Der öffentliche <hash>.0 Schlüssel befindet sich auch im LDLOGON-Verzeichnis und muss dort standardmäßig abgelegt sein. <Schlüsselname> ist der Zertifikatsname, der von Ihnen während des Setups der Management Suite angegeben wurde. Während des Setup ist es hilfreich, einen beschreibenden Schlüsselnamen als Schlüsselnamen anzugeben, wie z.B. den Namen des Core Servers (oder sogar dessen voll qualifizierten Namen). (Beispiel: ldcore oder ldcore.org.com). Dies vereinfacht die Identifizierung des Zertifikats/des privaten Schlüssels in einer Umgebung mit mehreren Cores.

Sie sollten vom Inhalt des Schlüsselverzeichnisses Ihres Core Servers eine Sicherungskopie anlegen. Wenn Sie aus irgendeinem Grund den Core Server neu installieren oder austauschen müssen, können Sie die Clients des betreffenden Core Servers solange nicht verwalten, bis Sie die Zertifikate des ursprünglichen Core wie unten beschrieben zum neuen Core hinzugefügt haben.

Gemeinsame Nutzung von Schlüsseln unter Core Servern

Clients kommunizieren nur mit Core und Rollup-Core Servern, für die sie eine übereinstimmende Datei für ein vertrauenswürdiges Zertifikat haben. Nehmen wir z.B. an, Sie setzen drei Core Server für die Verwaltung von je 5.000 Clients ein. Außerdem setzen Sie einen Rollup-Core Server für die Verwaltung aller 15.000 Clients ein. Jeder Core Server hat ein eigenes Zertifikat und private Schlüssel. Standardmäßig kommunizieren die Clientagenten, die Sie auf einem Core Server verteilen, nur mit dem Core Server, auf dem die Clientsoftware verteilt wird.

Es gibt zwei Hauptmethoden für die gemeinsame Schlüsselnutzung von Core und Rollup-Core Servern:

1. Verteilen des vertrauenswürdigen Zertifikats eines jeden Core Servers (die Datei <hash>.0) auf Clients und ihre jeweiligen Core Server. Dies ist die sicherste Methode.
2. Kopieren des privaten Schlüssels und der Zertifikate auf jeden Core Server. Auf den Clients müssen Sie hierzu keine Maßnahmen vornehmen. Da Sie jedoch den privaten Schlüssel kopieren müssen, ist das Risiko größer.

Wenn Sie in diesem Beispiel möchten, dass der Rollup-Core und die Webkonsole Clients von allen drei Cores verwalten, müssen Sie das vertrauenswürdige Zertifikat des Rollup-Cores (die Datei <hash>.0) auf alle Clients verteilen und dieselbe Datei in das Verzeichnis LDLOGON jeden Servers kopieren. Weitere Informationen finden Sie unter "Verteilen von vertrauenswürdigen Zertifikaten auf Clients" im nächsten Abschnitt.

Alternativ können Sie auch das Zertifikat/den privaten Schlüssel von jedem der drei Core Server auf den Rollup-Core kopieren. Auf diese Weise kann jeder Client den passenden privaten Schlüssel für seinen Core Server auf dem Rollup Core Server finden. Weitere Informationen finden Sie unter "Kopieren von Dateien für Zertifikate/private Schlüssel auf Core Server".

Wenn ein Core die Clients von einem anderen Core verwalten soll, können Sie dasselbe Verfahren anwenden und entweder das vertrauenswürdige Zertifikat auf Clients verteilen oder die Datei des Zertifikats/des öffentlichen Schlüssels unter den Cores verteilen.

Wenn Sie Zertifikate unter eigenständigen Core Servern (keine Rollup-Cores) kopieren, kommt noch folgendes Problem hinzu. Ein Core ist nicht in der Lage, die Clients eines anderen Core zu verwalten, es sei denn, er erhält vorab Zugriff auf einen Inventarscan der betreffenden Clients. Eine Möglichkeit, Inventarscans auf einen anderen Core zu übertragen, besteht darin, einen Auftrag für einen Inventarscan zu planen, der den Scan mithilfe einer benutzerdefinierten Befehlszeile an den neuen Core weiterleitet. In einer Konfiguration mit mehreren Core Servern ist die Verwendung eines Rollup-Core und der Webkonsole eine einfachere Möglichkeit, Clients über mehrere Cores hinweg zu verwalten. Rollup-Cores erhalten automatisch Inventarscan-Daten von allen Clients auf den Cores ab, für die ein Rollup durchgeführt wird.

Verteilen von vertrauenswürdigen Zertifikaten auf Clients

Es gibt zwei Methoden für die Verteilung von vertrauenswürdigen Zertifikaten auf Clients:

1. Verteilen einer Clientsetup-Konfiguration, die die gewünschten vertrauenswürdigen Zertifikate für Core Server umfasst.
2. Verwenden eines Softwareverteilungsauftrags, um die gewünschten Dateien für das vertrauenswürdige Zertifikat auf jeden Client zu kopieren.

Jedes zusätzliche vertrauenswürdige Zertifikat für Core Server (<hash>.0), das die Clients verwenden sollen, muss in das LDLOGON-Verzeichnis des Core Servers kopiert werden. Sobald sich das vertrauenswürdige Zertifikat in diesem Verzeichnis befindet, können Sie es auf der Authentifizierungsseite des Client-Setup-Assistenten auswählen. Das Clientsetup kopiert Schlüssel in dieses Verzeichnis auf Clients:

- Windows-Clients: \Programme\LANDesk\Shared Files\cbaroot\certs
- Mac OS X-Clients: /usr/LANDesk/common/cbaroot/certs

Wenn Sie das Zertifikat eines Core Servers zu einem Client hinzufügen möchten und Clientagenten nicht über ein Clientsetup neu verteilen möchten, erstellen Sie einen Softwareverteilungsauftrag, der < hash>.0 in das oben angegebene Verzeichnisse auf dem Client kopiert. Sie können dann das Fenster "Geplante Tasks" verwenden, um das von Ihnen erstellte Zertifikatsverteilungsskript zu verteilen.

Nachfolgend wird ein Beispiel eines benutzerdefinierten Skripts gezeigt, das zum Kopieren eines vertrauenswürdigen Zertifikats aus dem Verzeichnis LDLOGON des Core Servers auf einen Client verwendet werden kann. Ersetzen Sie hierzu d960e680 mit dem Hash-Wert für das vertrauenswürdige Zertifikat, das Sie verteilen möchten.

```
; Kopieren Sie ein vertrauenswürdiges Zertifikat aus dem Verzeichnis ldlogon des Core Servers

; in das Verzeichnis der vertrauenswürdigen Zertifikate des Clients

[MACHINES]

REMCOPY0=%DTMDIR%\ldlogon\d960e680.0, %TRUSTED_CERT_PATH%\d960e680.0
```

Kopieren von Dateien für Zertifikate/private Schlüssel auf Core Server

Eine Alternative zum Verteilen von Zertifikaten (<hash>.0) auf Clients ist das Kopieren von Sätzen aus Zertifikat/privatem Schlüssel unter den Cores. Cores können mehrere Dateien für Zertifikate/private Schlüssel umfassen. Sofern sich ein Client mit einem der Schlüssel auf einem Core authentifizieren kann, ist die Kommunikation mit diesem Core möglich.

Bei Verwendung der zertifikatsbasierten Fernsteuerung müssen sich die Zielclients in der Core-Datenbank befinden.
Wenn Sie die zertifikatsbasierte Fernsteuerungssicherheit auf Clients verwenden, lassen sich nur solche Clients fernsteuern, die über einen Inventardatensatz in der Core-Datenbank verfügen, mit der Sie verbunden sind. Vor der Kontaktaufnahme mit einem Knoten zwecks Eröffnung einer Fernsteuerungssitzung überprüft der Core die Datenbank, um sicherzustellen, dass der die Anfrage initiierende Teilnehmer berechtigt ist, den Client anzuzeigen. Wird der Client nicht in der Datenbank geführt, lehnt der Core die Anforderung ab.

So kopieren Sie einen Satz aus Zertifikat/privatem Schlüssel von einem Core Server auf einen anderen

1. Öffnen Sie auf dem Quell-Core Server den Ordner \Programme\LANDesk\Shared Files\Keys.
2. Kopieren Sie die Dateien <Schlüsselname>.key, <Schlüsselname>.crt und <hash>.0 des Quellservers auf eine Diskette oder an einen anderen sicheren Speicherort.
3. Kopieren Sie auf dem Ziel-Core Server die Dateien vom Quell-Core Server in denselben Ordner (\Programme\LANDesk\Shared Files\Keys). Die Schlüssel werden umgehend angewendet.

Gehen Sie umsichtig vor, damit der private Schlüssel <Schlüsselname>.key nicht gefährdet wird. Der Core Server verwendet diese Datei, um Clients zu authentifizieren, und jeder Computer mit der Datei <Schlüsselname>.key-Datei kann Remote-Ausführungen und Dateiübertragungen auf einen Management Suite-Client durchführen.

Erstellen einer Clientsetup-Konfiguration

Verwenden Sie den Client-Setup-Assistenten, um Client- und Serverkonfigurationen (wie die auf Clients installierten Komponenten oder die von Clientagenten verwendeten Netzwerkprotokolle) zu erstellen und zu aktualisieren.

Sie können Ihren Bedürfnissen entsprechend verschiedene Konfigurationen erstellen. Sie können beispielsweise Konfigurationen für die Clients in Ihrer Buchhaltung oder für Clients mit einem bestimmten Betriebssystem erstellen.

Um eine Konfiguration an Clients zu übermitteln, müssen Sie folgende Schritte ausführen:

- **Erstellen der Client-Setup-Konfiguration:** Richten Sie spezifische Konfigurationen für Ihre Clients ein.
- **Planen der Client-Konfiguration:** Übermitteln Sie die Konfiguration an Clients, auf denen der CBA oder der Fernsteuerungsagent installiert ist. Weitere Informationen finden Sie unter "Planen von Tasks" weiter unten in diesem Kapitel.

So erstellen Sie eine Clientkonfiguration

1. Klicken Sie in der Konsole auf **Extras | Clientsetup**.
2. Doppelklicken Sie auf das Symbol **Neue Konfiguration hinzufügen**.
3. Wählen Sie auf der Seite "Komponenten installieren" des Client-Setup-Assistenten die Komponenten aus, die Sie verteilen möchten.
4. Gehen Sie die verschiedenen Seiten durch, indem Sie auf **Weiter** klicken, und nehmen Sie die notwendigen Änderungen darin vor.
5. Wenn Sie diese Konfiguration als Standard einrichten möchten (die Konfiguration, die LDLOGON\IPSETUP.BAT installiert), klicken Sie auf **Als Standardkonfiguration festlegen**.
6. Klicken Sie auf **Fertigstellen**, um den Assistenten zu beenden.

Übermitteln einer Clientkonfiguration an einen bereits vorhandenen Agenten

Um eine Konfiguration an einen Client zu übermitteln, muss der CBA oder der Fernsteuerungsagent installiert sein. Möglicherweise hat ein anderes LANDesk-Produkt den CBA bereits installiert. Sie können Agenten auch über Anmeldeskripts auf einem Client installieren (weitere Informationen finden Sie im *Installations- und Verteilungshandbuch*).

Ehe Sie eine Clientkonfiguration planen, sollten sie das Netzwerk nach Clients durchsuchen, auf denen der CBA läuft, damit Sie eine aktuelle Liste erhalten.

So übermitteln Sie eine Clientkonfiguration an einen bereits vorhandenen Agenten

1. Klicken Sie in der Konsole auf **Extras | Clientsetup**.
2. Klicken Sie im Kontextmenü der Clientkonfiguration, die Sie per Push-Vorgang verteilen möchten, auf **Planen**.

3. Ziehen Sie den Client aus der Netzwerkansicht in das Fenster "Geplante Task". Ziehen Sie bei nicht verwalteten Geräten die Geräte aus dem Fenster "Nicht verwaltete Geräteerkennung" in das Fenster "Geplante Task".
4. Doppelklicken Sie in diesem Fenster auf den Task, um ein Anfangsdatum und eine Anfangszeit einzugeben. Beachten Sie, dass die ausgewählte Zeit von dem Core Server abhängt, auf dem der Scheduler-Dienst läuft. Sie können außerdem die Anzahl der erneuten Versuche angeben.
5. Wenn Sie fertig sind, klicken Sie auf **OK**. Es wird das Statusfenster "Geplanter Task" angezeigt.

Planen von Tasks

Sie können Tasks planen und sie an Clients übermitteln. Der Planungsdienst wird auf dem Core Server ausgeführt. Die Management Suite-Konsolen und die Webkonsolen können Tasks zum Scheduler hinzufügen. Im Fenster "Geplante Tasks" wird der Status von geplanten Tasks angezeigt und ob Tasks erfolgreich abgeschlossen werden konnten oder nicht. Sie können Berichte für geplante Tasks ausführen, um einen detaillierten Taskstatus zu erhalten.

Sie können die folgenden Tasktypen planen:

- Clientkonfigurationen
- Paketverteilungen
- Verschiedene benutzerdefinierte Skripts
- Benutzerdefinierte Datenformulare
- Nicht verwaltete Geräteerkennung

Jede Task ist mit einer ASCII-Skriptdatei verknüpft. Das Skript enthält Anweisungen für den Scheduler. Die meisten Skripts können Sie im Fenster "Skripte verwalten" verwalten (Extras | Skripte verwalten). Skripts sind im Verzeichnis LDMAIN\Scripts gespeichert.

Der Scheduler kann auf zwei Arten mit Clients kommunizieren:

- Über den CBA-Agenten (der bereits auf den Clients installiert sein muss).
- Über ein Systemkonto auf Domänenebene. Für das Konto, das Sie auswählen, muss die Anmeldung als Dienstprivileg gelten. Weitere Informationen zum Konfigurieren des Scheduler-Kontos finden Sie unter "Konfigurieren des Scheduler-Dienstes" in Kapitel 1.

Zuweisen von Zielen zu einem Task

Nachdem Sie ein Skript geplant haben, können Sie ihm Ziele zuweisen. Ziehen Sie Ziele von der Netzwerkansicht. Ziele können einzelne Clients, Computergruppen und Abfragen beinhalten. Abfragen und Gruppen sind leistungsstarke Optionen, mit deren Hilfe Sie dynamische Listen von Clients erstellen können, die sich für Routinetasks ändern lassen. Wenn sich z.B. die Clientzielliste einer Abfrage ändert, haben alle Tasks, die diese Abfrage verwenden, automatisch die neuen Clients zum Ziel.

Benutzeranzeige bei Ausführung von Tasks

Im Fenster "Geplante Tasks" wird stets der Auftragsstatus angezeigt. Wenn Sie Clientkonfigurationen oder Betriebssystem-Verteilungen planen, wird auch das Dialogfeld "Client Setup-Dienstprogramm" angezeigt. Während der Scheduler die Zielliste verarbeitet, werden die zu konfigurierenden Clients, Clients, die gerade konfiguriert werden sowie die abgeschlossenen Clients angezeigt. Weitere Informationen finden Sie unter "Informationen zum Dialogfeld "Clientsetup-Dienstprogramm"" weiter unten in diesem Kapitel.

Wenn Sie die Verteilung über Targeted Multicast planen, wird der Status im Fenster "Multicast Software Distribution" angezeigt. Dieses Fenster zeigt den Multicast-Status an. Weitere Informationen finden Sie unter "Info über das Fenster "Multicast Software Distribution"" in Anhang C.

In allen anderen Fällen wird das Fenster "Benutzerdefinierte Jobverarbeitung" angezeigt, das die geplanten, laufenden und abgeschlossenen Ziel-Clients sowie den Skriptstatus Zeile für Zeile anzeigt, während das Skript ausgeführt wird.

Anwenden von Bereichen auf geplante Tasks

Bei geplanten Tasks können mehrere Benutzer der Management Suite Ziele zu einem Task hinzufügen. Im Fenster "Geplante Tasks" werden jedem Benutzer der Management Suite jedoch nur die Ziele innerhalb seines Bereichs angezeigt. Wenn zwei Benutzer der Management Suite mit nicht überlappenden Bereichen jeweils 20 Ziele zu einem Task hinzufügen, werden jedem Benutzer der Management Suite nur die 20 Ziele angezeigt, die er hinzugefügt hat; der Task wird jedoch auf allen 40 Zielen ausgeführt.

Fenster "Geplante Tasks"

Im Fenster "Geplante Tasks" konfigurieren und planen Sie die Clientkonfiguration, die Paketverteilung und die Skript-Tasks. Planen Sie Elemente für eine einmalige Verteilung oder einen wiederkehrenden Task, z. B. einen Skript-Task für die regelmäßige Suche nach nicht verwalteten Geräten.

Das Fenster "Geplante Tasks" ist in zwei Hälften unterteilt. Im linken Bereich werden Task-Informationen angezeigt, im rechten Bereich werden Zielclientinformationen angezeigt.

Linker Bereich

Sie können Skripts auf den linken Bereich des Fensters "Geplante Tasks" ziehen. Sobald sich ein Skript im linken Bereich befindet, können Sie dafür Ziele konfigurieren, indem Sie Clients, Abfragen oder Gruppen auf den rechten Bereich ziehen.

- **Task:** Zeigt Task-Namen an.
- **Starten:** Zeitpunkt, zu dem die Ausführung des Task geplant ist. Doppelklicken Sie auf den Namen eines Task, um die Startzeit zu bearbeiten oder um eine Neuplanung durchzuführen.
- **Status:** Zeigt den Gesamtstatus des Task an. Weitere Details finden Sie im rechten Fensterausschnitt in den Spalten "Status" und "Ergebnis".

Rechter Bereich

- **Rechner:** Clients, auf denen der Task ausgeführt wird. Ziehen Sie sie von der Netzwerkansicht. Sie können auch Gruppen und Abfragen ziehen.
- **Status:** Gibt an, ob ein Auftrag wartet, fehlgeschlagen oder fertig ist.
- **Ergebnis:**Von dem Task zurückgegebene Meldungen.

Informationen zum Dialogfeld "Task planen"

Öffnen Sie dieses Dialogfeld im Fenster Extras | Geplante Tasks. Wählen Sie einen Task aus und klicken Sie auf die Schaltfläche **Startzeit festlegen** oder doppelklicken Sie auf einen Task im Fenster "Geplante Tasks".

Legen Sie in diesem Dialogfeld die Startzeit für den Task fest, ob der Task mehrmals ausgeführt werden soll und wenn ja, wie oft, und was geschehen soll, wenn der geplante Task nicht abgeschlossen werden kann.

Folgende Optionen stehen Ihnen im Dialogfeld "Geplante Tasks" zur Verfügung:

- **Jetzt starten:** Der Task wird gestartet, sobald Sie das Dialogfeld geschlossen haben. Der Start des Task kann sich um bis zu eine Minute verzögern.
- **Später starten:** Der Task wird zum angegebenen Datum und zur entsprechenden Uhrzeit gestartet.
- **Uhrzeit:** Der Task wird zur ausgewählten Uhrzeit gestartet. Standardmäßig enthält dieses Feld die aktuelle Uhrzeit.
- **Datum:** Der Task wird zum ausgewählten Datum ausgeführt. Geben Sie das Datum im Format MM/TT/JJ ein, oder öffnen Sie die Dropdown-Liste, um ein Datum aus dem Kalender auszuwählen.
- **Wiederholen alle:** Der Task wird in regelmäßigen Abständen wieder ausgeführt. Wählen Sie aus der Dropdown-Liste "Tag", "Woche" oder "Monat" aus, um festzulegen, wie häufig der Task ausgeführt werden soll. Er wird zur oben festgelegten Zeit wiederholt.
- **Nur fehlgeschlagene Computer neu planen:** Der Task wird nur für die Computer neu geplant, auf denen eine frühere Ausführung fehlgeschlagen ist.
- **Elemente aus Zwischenablage hinzufügen:** Elemente hinzufügen, die in der Netzwerkansicht ausgewählt und zur Zwischenablage (STRG+C) hinzugefügt wurden.
- **Anzahl der Wiederholungen:** Der Task wird so oft wiederholt, wie Sie es wünschen (wenn sie nicht abgeschlossen werden kann). Geben Sie einen Wert ein, oder verwenden Sie das Zahlenfeld.
- **Computer reaktivieren:** Ein heruntergefahrener Computer wird für die ausgewählte Task reaktiviert. Wenn der Task abgeschlossen ist, fährt sich der Computer selbst wieder herunter. Dies funktioniert nur bei Computern mit BIOS-Versionen, die die Wake-on-LAN-Technologie unterstützen. Aktivieren Sie diese Option nicht für Pull-Distributionspakete.

Informationen zum Dialogfeld Einen Task auswählen

Im Dialogfeld "Task auswählen" (**Extras | Geplante Tasks**, Symbolschaltfläche **Skript planen**) wählen Sie einen Task aus und führen diesen aus. Gegenwärtig kann die Konsole folgende Skript-Tasks enthalten:

- **am_verifyall:** Alle Pakete, die über Richtlinien auf Clients installiert wurden, werden überprüft.
- **Beispiel dir-Befehl:** Führt ein Betriebssystem-Verteilungsskript aus, um zu demonstrieren, wie ein Client mit einem virtuellen Datenträger neu gestartet und ein dir-Befehl ausgeführt wird.
- **inventoryscanner:** Der Inventarscanner wird für ausgewählte Clients ausgeführt.

- **multicast_domain_discovery:** Es wird eine Multicast-Domänenrepräsentantenerkennung ausgeführt. Weitere Informationen finden Sie unter "Verwenden von Targeted Multicasting mit Enhanced Software Distribution" in Kapitel 6.
- **multicast_info:** Es wird ein Problembehandlungsskript ausgeführt, das anzeigt, welche Informationen das Fenster "Geplante Tasks" an Targeted Multicast weitergibt, einschließlich der IP-Adressen des Ziel-Client sowie Subnetzinformationen. Die Datei C:\MCINFO.TXT wird erstellt.
- **MSI-Dienst-Verteilung:** Es wird der MSI-Dienst verteilt, der für einen PXE-Repräsentanten erforderlich ist.
- **PXE-Repräsentantenverteilung:** Ein PXE-Repräsentant wird verteilt oder aktualisiert.
- **PXE-Repräsentantenentfernung:** Die PXE-Dienstsoftware wird von einem PXE-Repräsentanten entfernt.
- **Clientdatensätze wiederherstellen:** Führt den Inventarscanner auf ausgewählten Clients aus, der Scanner macht jedoch an den Core Meldung, von dem der Client aus konfiguriert wurde. Wenn Sie die Datenbank zurücksetzen müssen, hilft Ihnen dieser Task, die Clients in einer Umgebung mit mehreren Cores wieder der richtigen Datenbank zuzuordnen.
- **Überwachungsclient deinstallieren:** Entfernt den Softwareüberwachungsclient auf Zielcomputern. Dieser Client wurde in Management Suite vor Version 7 eingesetzt.

Im Fenster "Skripte verwalten" (**Extras | Skripte verwalten**) können Sie Task-Optionen bearbeiten.

Sie müssen folgende Schritte ausführen, bevor Sie Tasks für einen Client planen können:

- Starten Sie den Intel Scheduler-Dienst auf dem Core Server. Dieser Dienst startet automatisch, wenn die Konsole korrekt installiert ist.
- Starten Sie den Intel Ping Discovery Service (PDS) auf dem Core Server und den Clients. Dieser Dienst startet automatisch, wenn die Konsole korrekt installiert ist.
- Scannen Sie den Client in die Core-Datenbank. Wenn Sie einen Client zum ersten Mal konfigurieren, werden die Diagnosedaten gescannt und automatisch in der Core-Datenbank registriert.

Die Konsole enthält Skripts, die Sie planen können, um Routinewartungs-Tasks wie die Ausführung von Inventarscans auf ausgewählten Computern durchzuführen. Sie weisen die Skripts im Fenster "Geplante Tasks" zu und planen sie genauso wie andere Tasks.

Skripts sind Windows .INI-Dateien, die Sie mit jedem Texteditor bearbeiten und im Verzeichnis \Programme\LANDesk\ManagementSuite\Scripts auf Ihrem Core Server speichern können. Wenn Sie die Optionen in einer Skript-Task ändern müssen, öffnen Sie das entsprechende Skript und befolgen Sie die darin enthaltenen Anweisungen.

So planen Sie ein Skript

1. Klicken Sie im Fenster **Skripte verwalten** auf **Skripte > Eigene Skripte** oder **Alle anderen Skripte** und auf das Skript, das Sie verteilen möchten.
2. Klicken Sie auf die Schaltfläche **Task erstellen**. Anschließend wird das Fenster **Geplante Tasks** mit dem von Ihnen ausgewählten Skript angezeigt.
3. Suchen Sie in der Netzwerkansicht nach den Clients, die aktualisiert werden sollen, und verschieben Sie ihre Symbole mittels Ziehen-und-Ablegen in den rechten Bereich des Fensters **Geplante Tasks**.
4. Klicken Sie im Fenster **Geplante Tasks** auf die Symbolschaltfläche **Startzeit festlegen**, um das Dialogfeld **Task planen** anzuzeigen.
5. Legen Sie die gewünschten Zeitoptionen fest. Klicken Sie auf **Jetzt starten** und auf **OK**, wenn die Aktualisierung des Clients so bald wie möglich erfolgen soll.

Konfigurieren lokaler Scheduler-Skripte

Der lokale Scheduler ist ein Dienst, der auf Clientcomputern ausgeführt wird. Sie können ihn über das Clientsetup installieren. Im Allgemeinen ist der lokale Scheduler für Management Suite-Aufgaben zuständig, wie z.B. die Ausführung des Inventarscanners in regelmäßigen Abständen. Andere zeitplangesteuerte Tasks, wie z.B. Software- oder Betriebssystemverteilungen, werden anstatt vom lokalen Scheduler vom Core Server ausgeführt. Sie können mit dem lokalen Scheduler eigene Tasks für die periodische Ausführung auf Clients planen. Sobald Sie ein lokales Scheduler-Skript erstellt haben, können Sie es mithilfe des Fensters "Geplante Tasks" auf den relevanten Clients verteilen.

Der lokale Scheduler weist jedem Task eine Kennnummer zu. Der Kennungsbereich der lokalen Scheduler-Skripte unterscheidet sich von den Standardskripten des lokalen Schedulers, mit denen die Management Suite arbeitet. Standardmäßig darf auf jedem Client immer nur ein benutzerdefiniertes Scheduler-Skript aktiv sein. Wenn Sie ein neues Skript erstellen und auf Clients verteilen, ersetzt das neue Skript das alte Skript (jedes Skript im benutzerdefinierten Kennungsbereich des Local Scheduler), ohne sich auf die Standardskripte des Local Scheduler (beispielsweise den Zeitplan für den lokalen Inventarscan) auszuwirken.

Folgende Optionen stehen Ihnen im Dialogfeld "Local Scheduler" zur Verfügung:

- **Befehl** Geben Sie das Programm ein, das Sie lokal ausführen möchten. Geben Sie den vollständigen Pfad zum Programm ein oder stellen Sie sicher, dass sich das Programm in einem Ordner befindet, der im Pfad des Clients enthalten ist. Dieser Pfad muss auf allen Clients gleich sein, auf denen Sie dieses Skript bereitstellen.
- **Parameter:** Geben Sie an das Programm weiterzuleitende Befehlszeilenparameter ein.
- **Häufigkeit:** Wählen Sie das Wiederholungsintervall, wenn der Task wiederholt ausgeführt werden soll.
- **IP-Adresse geändert:** Aktivieren Sie diese Option, wenn der Task nur ausgeführt werden soll, wenn sich die IP-Adresse des Clients ändert. Verwenden Sie diese Option, um bei einer Änderung der IP-Adresse einen Inventarscan zu veranlassen und die IP-Adresse in der Management Suite-Datenbank synchron zu halten.
- **Benutzer ist angemeldet:** Aktivieren Sie diese Option, um den Task nur auszuführen, wenn der Benutzer angemeldet ist.
- **Bandbreite:** Aktivieren Sie diese Option, um die für die Ausführung des Tasks erforderliche Mindestbandbreite anzugeben (RAS, WAN oder LAN). Sie können auch angeben, welcher Computer als Ziel für den Bandbreitentest zwischen Ziel und Client dienen wird.
- **Startzeit:** Aktivieren Sie diese Option, um festzulegen, nach welchem Datum und welcher Uhrzeit der Task aktiv sein soll. Wenn Sie eine anderen Optionen konfigurieren, wird der Task zu der von Ihnen festgelegten Startzeit ein Mal ausgeführt.
- **Tageszeit:** Aktivieren Sie diese Option, um einen Uhrzeitbereich für die Ausführung des Task festzulegen.
- **Wochentag:** Aktivieren Sie diese Option, um einen Wochentagbereich für die Ausführung des Task festzulegen.
- **Monatsdatum:** Aktivieren Sie diese Option, um einen Tag des Monats für die Ausführung des Task festzulegen.

Gehen Sie bei der Auswahl der Zeitplanoptionen nicht so restriktiv vor, dass die Kriterien für den Task selten erfüllt werden, es sei denn, dass ist Ihre Absicht. Beispiel: Wenn Sie beim Konfigurieren eines Task als Wochentag den Montag auswählen und den 17. als Tag des Monats, wird der Task nur an einem Montag ausgeführt, der auch gleichzeitig der 17. des Monats ist; dieser Fall tritt jedoch nur sehr selten ein.

So konfigurieren Sie einen Befehl im Local Scheduler

1. Erstellen Sie im Fensterbereich "Verwaltete Skripte" (**Extras | Verwaltete Skripte**) ein neues Local Scheduler-Skript.
2. Geben Sie einen **Skriptnamen** ein.
3. Klicken Sie auf **Hinzufügen**, um die Optionen für das Skript zu definieren.
4. Konfigurieren Sie die Local Scheduler-Optionen wie bereits beschrieben.
5. Klicken Sie auf **Speichern**, um Ihr Skript zu speichern.
6. Stellen Sie das von Ihnen erstellte Skript mithilfe des Fensterausschnitts "Geplante Tasks" auf den Clients zur Verfügung.

Erläuterungen zu den Bandbreitenoptionen

Beim Konfigurieren von Local Scheduler-Befehlen können Sie angeben, welche Bandbreitenkriterien mindestens erfüllt sein müssen, damit der Task ausgeführt werden kann. Der Bandbreitentest besteht aus Daten, die durch das Netzwerk zu dem Computer fließen, der von Ihnen angegeben wurde. Zu dem Zeitpunkt, zu dem der Task ausgeführt werden soll, sendet jeder Client, der den Local Scheduler-Task ausführt, eine kleine Menge ICMP-Netzwerkdaten an den von Ihnen angegebenen Computer und wertet die Übertragungsleistung aus. Wenn der Zielcomputer für den Test nicht verfügbar ist, wird der Task nicht ausgeführt.

Sie können folgende Bandbreitenoptionen auswählen:

- **RAS:** Der Task wird ausgeführt, wenn die Netzwerkverbindung des Clients mit dem Zielcomputer mindestens RAS- oder DFÜ-Geschwindigkeit erreicht. Diese Option auszuwählen bedeutet im Allgemeinen, dass der Task immer ausgeführt wird, wenn der Client über irgendeine Netzwerkverbindung verfügt.
- **WAN:** Der Task wird ausgeführt, wenn die Verbindung des Clients mit dem Zielcomputer mindestens WAN-Geschwindigkeit erreicht. Die LAN-Geschwindigkeit ist standardmäßig als 262.144 Bit/s definiert.
- **LAN:** Der Task wird ausgeführt, wenn die Verbindung des Clients mit dem Zielcomputer die LAN-Geschwindigkeitseinstellung überschreitet.

Verwenden von "Nicht verwaltete Geräteerkennung"

Die "Nicht verwaltete Geräteerkennung" (UDD) ist eine Neuerung der Management Suite 8. UDD findet Clients in Ihrem Netzwerk, die keinen Inventarscan an die Management Suite Core-Datenbank gesendet haben. UDD findet nicht verwaltete Clients auf verschiedene Weise.

- **CBA-Erkennung:** Es wird nach dem LANDesk CBA-Agenten gesucht. Mit dieser Option werden Computer gefunden, die über Management Suite, LANDesk Client Manager, LANDesk System Manager und so weiter verfügen.
- **Netzwerkscan:** Mithilfe einer ICMP-Ping-Suche wird nach Computern gesucht. Diese Suche ist am gründlichsten, aber auch am langsamsten. Sie können die Suche auf bestimmte IP- und Subnetzbereiche beschränken. Standardmäßig verwendet diese Option NetBIOS, um Daten über das Gerät zu sammeln. Ihnen steht auch die Option "IP-Fingerabdruck" zur Verfügung; hierbei versucht UDD die Betriebssystemart über TCP-Paketantworten herauszufinden Diese Option verlangsamt die Suche geringfügig.
- **Windows NT-Domäne:** In einer von Ihnen angegebenen Domäne wird nach Clients gesucht. Die Mitglieder werden unabhängig davon, ob der Computer an- oder ausgeschaltet ist, gefunden.
- **LDAP-Verzeichnis:** In einem von Ihnen angegebenen Verzeichnis wird nach Clients gesucht. Die Mitglieder werden unabhängig davon, ob der Computer an- oder ausgeschaltet ist, gefunden.

Um die Suche nach nicht verwalteten Clients zu automatisieren, können Sie regelmäßige Suchen planen. Sie können beispielsweise Ihr Netzwerk in Drittel einteilen und für jedes Drittel eine Ping-Suche pro Nacht planen.

Wenn Sie eine Erkennung planen, übernimmt diese der Core Server. Ungeplante Erkennungen gehen von der Konsole aus, die sie startet.

So werden nicht verwaltete Geräte erkannt

1. Klicken Sie im Fenster "Nicht verwaltete Geräteerkennung" auf (**Extras | Nicht verwaltete Geräteerkennung**) und klicken Sie dann auf die Schaltfläche **Netzwerk scannen**.
2. Wählen Sie die gewünschte Erkennungsart aus.
3. Geben Sie einen Anfangs- und End-IP-Bereich für den Scan ein. Sie müssen einen Bereich für die **CBA-Erkennung** oder die **Netzwerkerkennung** eingeben. Der Bereich ist optional für **NT-Domäne** und **LDAP**.
4. Geben Sie eine **Subnetzmaske** ein.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den gerade konfigurierten Scan zur Taskliste hinzuzufügen.
6. Wählen Sie in der Taskliste unten im Dialogfeld die Scans aus, die Sie durchführen möchten, und klicken Sie auf die Schaltfläche **Jetzt scannen**, um den Scan sofort durchzuführen bzw. auf die Schaltfläche **Task planen**, um die Scans später oder auf der Basis eines wiederkehrenden Plans auszuführen. Die Schaltflächen **Jetzt scannen** und **Task planen** führen nur Scans aus, die Sie zur Taskliste hinzugefügt haben und die ausgewählt sind.

7. Aktualisierungen des Scanstatus werden im Fenster "Scanstatus" angezeigt. Wenn der Scan beendet ist, klicken Sie in den Dialogfeldern "Scanstatus" und "Scannerkonfiguration" auf **Schließen**.
8. Klicken Sie in der UDD-Struktur auf **Computer**, um die Scanergebnisse anzuzeigen.

Konfigurieren der Windows NT-Domänenerkennung

Die Windows NT-Domänenerkennungsoption von UDD funktioniert nur, wenn Sie den Scheduler-Dienst so konfigurieren, dass er sich bei der Domäne mit einem Domänenadministratorkonto anmeldet.

So konfigurieren Sie das Scheduler-Anmeldekonto

1. Klicken Sie auf **Konfigurieren | Dienste** und anschließend auf das Register **Scheduler**.
2. Klicken Sie auf **Anmeldedaten ändern**.
3. Geben Sie einen Domänenadministrator-Benutzernamen und ein Kennwort ein.
4. Klicken Sie auf **OK**
5. Starten Sie den Scheduler-Dienst neu, damit die Änderungen übernommen werden. Klicken Sie im Register "Scheduler" auf **Stopp** und auf **Start**, wenn der Dienst gestoppt wurde.

Was geschieht, wenn UDD ein nicht verwaltetes Gerät findet?

Wenn UDD ein nicht verwaltetes Gerät zum ersten Mal findet, versucht sie, den Gerätetyp zu identifizieren, um ihn einer der folgenden vier Kategorien zuordnen zu können:

- **Computer:** Umfasst Computer
- **Infrastruktur:** Umfasst Router und andere Netzwerk-Hardware
- **Sonstiges:** Umfasst nicht identifizierte Geräte
- **Drucker:** Umfasst Drucker.

Dank dieser vier Kategorien bleibt die UDD-Liste strukturiert, und Sie finden die Geräte, für die Sie sich interessieren, leichter. Sie können die Geräteliste nach jeder Spaltenüberschrift sortieren, indem Sie darauf klicken. UDD stuft die Geräte möglicherweise nicht immer richtig ein. Sie können falsch identifizierte Geräte einfach in die korrekte Gruppe ziehen.

UDD versucht, für jedes Gerät die folgenden grundlegenden Daten zu finden:

- **Gerätename:** Der ermittelte Gerätename, falls vorhanden.
- **IP-Adresse:** Die ermittelte IP-Adresse. UDD zeigt sie immer an.
- **Subnetzmaske:** Die ermittelte Subnetzmaske. UDD zeigt sie immer an.
- **Betriebssystembeschreibung:** Die ermittelte Betriebssystembeschreibung, falls vorhanden.
- **MAC-Adresse:** Die ermittelte MAC-Adresse; diese wird üblicherweise zurückgegeben, wenn das Gerät über CBA oder NetBIOS verfügt bzw. wenn sich das Gerät auf demselben Subnetz wie der Core Server oder die Konsole befindet, der/die die Suche durchführt.

- **Gruppe:** Die UDD-Gruppe, zu der das Gerät gehört.
- **CBA:** Gibt an, ob das Gerät über CBA verfügt. "J" in der Spalte bedeutet Ja, "N" bedeutet Nein. Sie können den Management Suite-Client direkt an Geräte verteilen, die CBA geladen haben.
- **Alle Benutzer:** Am überprüften Gerät angemeldete Benutzer, falls vorhanden.
- **Gruppe/Domäne:** Die Gruppe/Domäne, der das Gerät angehört, falls vorhanden.
- **Zuerst geprüft:** Das Datum, an dem UDD das Gerät zum ersten Mal überprüft hat.
- **Zuletzt geprüft:** Das Datum, an dem UDD das Gerät zum letzten Mal überprüft hat. Mithilfe dieser Spalte finden Sie nicht verwaltete Geräte, die sich nicht mehr im Netzwerk befinden, oder die erst vor kurzem gefunden wurden.
- **Geprüfte Male:** Gibt an, wie oft UDD dieses Gerät überprüft hat.

Abhängig vom Gerät, kann UDD möglicherweise nicht für alle Spalten Daten liefern. Wenn UDD ein Gerät zum ersten Mal findet, sucht sie in der Core-Datenbank nach der IP-Adresse und dem Namen des Geräts. Wenn diese Daten bereits in der Datenbank enthalten sind, ignoriert UDD das Gerät. Sind diese Daten noch nicht vorhanden, so fügt UDD das Gerät zur Tabelle der nicht verwalteten Geräte hinzu. In dieser Tabelle enthaltene Geräte verwenden keine Management Suite-Lizenz. Ein Gerät gilt als verwaltet, wenn es einen Inventarscan an die Core-Datenbank sendet. Sie können Geräte nicht aus UDD in die Hauptkonsolen-Netzwerkansicht ziehen. Sobald nicht verwaltete Geräte einen Inventarscan gesendet haben, werden Sie aus UDD entfernt und automatisch der Netzwerkansicht hinzugefügt.

Wenn nicht alle Spalten zu einem gefundenen Gerät Daten enthalten, können Sie das Gerät auswählen und auf **IP-Fingerabdruck vornehmen** klicken. UDD sendet eine Reihe von Paketen an das Gerät und versucht, basierend auf den Antworten weitere Daten zu sammeln. Abhängig vom Gerät und der Betriebssystemart, findet "IP-Fingerabdruck" unterschiedliche Daten.

Sie können Gruppen erstellen, um nicht verwaltete Geräte weiter einzustufen. Wenn Sie ein Gerät in eine andere Gruppe verschieben, lässt UDD es bei einer späteren Erkennung in dieser Gruppe. Es ist wichtig, die Hauptgruppe der **Computer** gut zu organisieren und über Geräte, die Sie nicht mit Management Suite verwalten möchten, in Untergruppen oder andere Kategorien zu verschieben. So können Sie neue Geräte in der Gruppe **Computer** leicht erkennen. Wenn Sie eine Gruppe, die Geräte enthält, löschen, verschiebt UDD die Geräte in die Gruppe **Sonstige**.

Über das Feld "Suchen" in der Symbolleiste können Sie schnell Geräte finden, die von Ihnen angegebenen Suchkriterien entsprechen. Sie können nach Daten in einer bestimmten Spalte oder in allen Spalten suchen. Die Suchergebnisse werden in der Kategorie "Ergebnisse suchen" angezeigt. Sie können beispielsweise über "Suchen" nicht verwaltete Computer gruppieren, die CBA haben, indem Sie nach dem Wert "J" im Feld "CBA" suchen.

Sie können auch einen AMS-Alarm erstellen, wenn UDD nicht verwaltete Geräte findet. Der in AMS zu konfigurierende Alarmname lautet **Nicht verwaltetes Gerät gefunden**.

Verteilung an nicht verwaltete Geräte

Sie können Management Suite-Agenten wie folgt an nicht verwaltete Geräte verteilen:

- Über Push-basierte Verteilungen mithilfe von "Geplante Aufgaben" und einem Domänenverwaltungskonto, das Sie für den Scheduler konfiguriert haben. Funktioniert bei Windows NT-/2000-/2003-/XP-Clients.
- Über Push-basierte Verteilungen mithilfe von CBA. Wenn die Clients über CBA verfügen, können Sie eine Push-basierte Verteilung verwenden.
- Über eine Pull-basierte Verteilung mithilfe eines Anmeldeskripts.

Weitere Informationen zum Verteilen von Clients finden Sie in Stufe 4 im *Installations- und Verteilungshandbuch*.

Wenn Sie Clients für die Agentenverteilung organisieren, ist es einfacher, die Liste der nicht verwalteten Geräte für CBA-Gruppenverteilungen nach CBA und für Geplante Aufgaben-Verteilungen nach Domäne zu sortieren.

Verteilung auf Windows XP-Clients
Die Standardeinstellungen von Windows XP erzwingen, dass Netzwerkanmeldungen, die ein lokales Konto für die Anmeldung verwenden, sich stattdessen mit einem Gästekonto anmelden. Wenn Sie ein Administratorkonto auf Domänenebene und ein lokales für den Scheduler-Dienst verwenden, schlagen geplante Tasks fehl, weil der Scheduler-Dienst die Authentifizierung nicht durchführen kann. Weitere Informationen finden Sie unter "Stufe 4: Verteilen der primären Agenten auf Clients" im *Installations- und Verteilungshandbuch*.

So verteilen Sie Agenten auf nicht verwaltete Geräte

1. Klicken Sie auf **Extras| Clientsetup** und erstellen Sie eine neue Konfiguration, oder verwenden Sie eine vorhandene Konfiguration. Klicken Sie im Kontextmenü der Konfiguration auf **Planen**.
2. Klicken Sie auf **Extras | Nicht verwaltete Geräte** und wählen Sie die Geräte aus, an die Agenten verteilt werden sollen. Ziehen Sie die Geräte in das Fenster "Geplante Tasks". Wenn das Fenster "Geplante Tasks" eine minimierte Registerkarte ist, können Sie die Geräte auf die Registerkarte "Geplante Tasks" ziehen. Hierbei wird das Fenster "Geplante Tasks" geöffnet.
3. Wenn die Geräte nicht über CBA verfügen, klicken Sie auf **Konfigurieren | Dienste** und anschließend auf die Registerkarte **Scheduler**. Stellen Sie sicher, dass das Scheduler-Konto auf den Geräten, auf die Sie Agenten verteilen möchten, über Administratorrechte verfügt.
4. Doppelklicken Sie auf das Verteilungsskript und legen Sie eine Startzeit fest. Klicken Sie auf **OK**, wenn Sie fertig sind.
5. Überprüfen Sie das Fenster "Geplante Tasks" auf Aktualisierungen.

Wiederherstellen von Clientdatensätzen

Sollten Sie jemals Ihre Core-Datenbank zurücksetzen und gezwungen sein, Clientdaten wiederherzustellen, können Sie mithilfe von UDD alle Clients auf dem Netzwerk erkennen lassen. Anschließend können Sie die Ergebnisse des Erkennungsvorgangs als Ziel für den geplanten Task "Clientdatensätze wiederherstellen" verwenden. Wenn der CBA-Agent auf den Clients installiert ist, veranlasst dieser Task, dass die Clients einen vollständigen Inventarscan an die Core-Datenbank senden, für die jeder Client lokal konfiguriert ist. Dieser Task veranlasst, dass diejenigen Clients, die bereits konfiguriert sind, zurück in die Datenbank gescannt werden und die Clients immer noch auf den für sie zuständigen verwaltenden Core Server zeigen. Der Task misslingt auf Clients, die nicht von einem Core Server verwaltet wurden.

So stellen Sie Clientdatensätze wieder her

1. Verwenden Sie UDD - wie bereits beschrieben - zur Erkennung nicht verwalteter Geräte.
2. Klicken Sie auf **Extras | Geplante Tasks**.
3. Klicken Sie im Fensterausschnitt "Geplante Tasks" auf die Schaltfläche **Skript planen**.
4. Klicken Sie auf **Clientdatensätze wiederherstellen** und dann auf **OK**.
5. Ziehen Sie die wiederherzustellenden Computer aus der UDD-Strukturansicht "Ergebnisse suchen" in den rechten Bereich des Fensters "Geplante Tasks".
6. Doppelklicken Sie auf das Skript und legen Sie eine Startzeit fest. Klicken Sie auf **OK**, wenn Sie fertig sind.
7. Überprüfen Sie das Fenster "Geplante Tasks" auf Aktualisierungen.

Informationen zum Dialogfeld "Scannerkonfiguration"

Im Dialogfeld "Scannerkonfiguration" (**Extras | Nicht verwaltete Geräteerkennung**, Schaltfläche **Scannerkonfiguration**) können Sie Scans für nicht verwaltete Geräte Ihren Bedürfnissen anpassen und anschließend ausführen.

- **Gespeicherte Konfigurationen:** Die gespeicherten Scannerkonfigurationen werden angezeigt. Sie speichern eine Konfiguration, indem Sie die gewünschten Änderungen an den Einstellungen vornehmen, auf **Neu** klicken, die Konfiguration benennen, diese auswählen und anschließend auf **Speichern** klicken.
- **CBA-Erkennung:** Clients, auf denen der CBA-Agent läuft, werden gefunden. Wenn Ihre Clients über CBA verfügen, ist dies die schnellste Suchmethode.
    - **PDS2-Erkennung:** Geräte, die den älteren LANDesk PDS2-Agent verwenden, werden gefunden. Sie können diese Option nur wählen, wenn Sie zuerst **CBA-Erkennung** ausgewählt haben.
- **Netzwerkscan:** Geräte werden mithilfe einer ICMP-Ping-Suche gefunden. Diese Suchmethode ist die genaueste und langsamste.
    - **IP-Fingerabdruck:** Gerätedaten wie Betriebssystemart, angemeldete Benutzer, Domäne usw. werden, wenn vorhanden, gefunden. Abhängig von der gefundenen Geräteart und dem Betriebssystem, findet UDD unterschiedliche Daten. Diese Option verlangsamt die Suche etwas, da UDD speziell erstellte Pakete an die gefundenen Geräte versendet und die Antworten analysiert.

- **NT-Domäne:** Geräte in einer Windows NT-Domäne werden gefunden. Diese Option verwendet die NT-Domänen-Kontodaten und benötigt keinen IP-Adressenbereich; Sie können jedoch einen solchen angeben. Wenn Sie diese Option wählen und auf **Konfigurieren** klicken, wird das Dialogfeld "NT-Domänenkonfiguration" angezeigt; dort können Sie die NT-Domänen-Erkennungseinstellungen Ihren Bedürfnissen anpassen.
- **Nach IP-Bereich filtern** (für NT-Domäne und LDAP): NT-Domäne und LDAP-Erkennung werden nach den IP-Bereichen gefiltert, die Sie unter**Erste IP-Adresse** und **Letzte IP-Adresse** angegeben haben.
- **LDAP:** Geräte in einem LDAP-Verzeichnis werden gefunden. Wenn Sie diese Option wählen und auf **Konfigurieren** klicken, wird das Dialogfeld "LDAP-Konfiguration" angezeigt; dort können Sie die LDAP-Erkennungseinstellungen Ihren Bedürfnissen anpassen.
- **Erste IP-Adresse:** Geben Sie die Start-IP-Adresse für den Adressenbereich ein, den Sie überprüfen möchten.
- **Letzte IP-Adresse:** Geben Sie die End-IP-Adresse für den Adressenbereich ein, den Sie überprüfen möchten. UDD aktualisiert dieses Feld automatisch, während Sie die **Erste IP-Adresse** eingeben; Sie können die letzte IP-Adresse aber auch manuell ändern. **Letzte IP-Adresse** wird aus dem Wert im Feld **Subnetzmaske** und dem Wert im Feld **Erste IP-Adresse** berechnet.
- **Subnetzmaske:** Geben Sie die Subnetzmaske für den IP-Adressenbereich ein, den Sie überprüfen.
- **Hinzufügen** und **Entfernen:** Fügt die IP-Adressenbereiche zur Arbeitsschlange unten im Dialogfeld hinzu oder entfernt sie daraus.
- **Task planen:** Der Scan wird basierend auf Ihren Einstellungen geplant. Sie können die Startzeit im Fenster "Geplante Tasks" anpassen. Geplante Scans gehen vom Core Server aus.
- **Jetzt scannen:** Der Scan wird, basierend auf Ihren Einstellungen, sofort gestartet. Hier gestartete Scans gehen von der aktuellen Konsole aus. Sobald Sie den Scan gestartet haben, wird das Dialogfeld "Scanstatus" angezeigt. Es zeigt die Gesamtzahl der gefundenen Geräte an, wie viele vorhandene Geräte aktualisiert wurden und wie viele neue nicht verwaltete Geräte hinzugefügt wurden.

Informationen zum Dialogfeld "NT-Domänenkonfiguration"

In diesem Dialogfeld konfigurieren Sie die Verbindung zu der Domäne, die Sie überprüfen möchten.

- **Domäne:** Geben Sie die Domäne ein, die Sie überprüfen möchten.
- **Als aktueller Benutzer anmelden:** Wählen Sie diese Möglichkeit, wenn Sie als Benutzer mit Zugriff auf die Domäne, die Sie überprüfen, angemeldet sind.
- **Anmelden als:** Wählen Sie diese Möglichkeit, wenn Sie nicht als Benutzer mit Zugriff auf die Domäne, die Sie überprüfen, angemeldet sind. Geben Sie außerdem einen **Benutzernamen** und ein **Kennwort** ein.
- **Hinzufügen** und **Entfernen:** Fügen Sie jede Domäne, die Sie konfigurieren und die Sie überprüfen möchten, zur Arbeitsschlange hinzu, indem Sie auf **Hinzufügen** klicken. Klicken Sie auf **Entfernen**, um eine ausgewählte Domäne aus der Arbeitsschlange zu löschen.

Informationen zum Dialogfeld "LDAP-Konfiguration"

In diesem Dialogfeld konfigurieren Sie die Verbindung zu dem LDAP-Verzeichnis, das Sie überprüfen möchten.

- **LDAP://:** Geben Sie das LDAP-Verzeichnis ein, das Sie überprüfen möchten.
- **Als aktueller Benutzer anmelden:** Wählen Sie diese Möglichkeit, wenn Sie als Benutzer mit Zugriff auf das Verzeichnis, das Sie überprüfen, angemeldet sind.
- **Anmelden als:** Wählen Sie diese Möglichkeit, wenn Sie nicht als Benutzer mit Zugriff auf das Verzeichnis, das Sie überprüfen, angemeldet sind. Geben Sie außerdem einen **Benutzernamen** und ein **Kennwort** ein.
- **Einzelne OUs auswählen:** Wählen Sie die OUs aus, die Sie überprüfen möchten. Klicken Sie auf **Hinzufügen**, um sie zur Arbeitsschlange hinzuzufügen. Klicken Sie auf **Entfernen**, um die ausgewählte OU aus der Arbeitsschlange zu löschen.
- **Aktiver Verzeichnispfad:** Der aktive Verzeichnispfad wird angezeigt, falls vorhanden.

Verwenden von LANDesk Server Manager und LANDesk-Systemverwalter mit der LANDesk Management Suite

Server Manager und Systemverwalter sind unabhängig voneinander über die LANDesk-Software verfügbar und in die Management Suite integriert. Zum Lieferumfang von Management Suite gehören eine Serverlizenz und die von Ihnen erworbene Anzahl von Clientlizenzen. Zur Installation von Management Suite-Agenten auf einem Serverbetriebssystem erfordert Management Suite eine zusätzliche Serverlizenz für jeden Server. Server Manager fügt Management Suite-Serverlizenzen hinzu, zusätzlich zu Server Manager-spezifischen Funktionen für verwaltete Server.

Der Systemverwalter unterstützt Sie bei der Verwaltung von Clients auf dem Netzwerk und bei der Fehlerbehebung von allgemeinen Computerproblemen, bevor diese zu ernsthaften Problemen führen. Wenn sich Clients im Netzwerk befinden, die bereits mit dem Systemverwalter verwaltet werden, können Sie die Systemverwalterintegration der Management Suite verwenden, um diese Computer über die Management Suite-Konsole zu verwalten.

Verteilen von Server Manager und Systemverwalter auf Clients

Nachdem Sie Server Manager und/oder den Systemverwalter auf dem Core Server installiert haben, sind im Fenster "Clientsetup" zwei Konfigurationssymbole verfügbar: die Schaltfläche **Serverkonfiguration hinzufügen** sowie **Clientkonfiguration hinzufügen**. Die Optionen und Standardeinstellungen der beiden Konfigurationen unterscheiden sich geringfügig.

- Mit der Option **Serverkonfiguration hinzufügen** können Sie die Serverversion des System Manager-Clients sowie eine Version der Fernsteuerung installieren, die auf der Anwendungsebene anstatt der Treiberebene läuft. Dadurch werden Fernsteuerungsprobleme vermieden, die zu einem Absturz Ihres Servers führen können; die Leistung ist jedoch geringfügig eingeschränkt. Die System Manager-spezifischen Optionen bei dieser Clientsetup-Art sind **System Manager (Server)** und **Fernsteuerung für Server**.
- Mit der Option **Clientkonfiguration hinzufügen** können Sie die Clientversion des System Managers sowie alle anderen Komponenten der Management Suite installieren. Die System Manager-spezifischen Optionen in dieser Client Setup-Art sind **System Manager** für Desktop-Clients und **Mobile Manager-Unterstützung** für mobile Clients.

Die System Manager-Agenten arbeiten erst nach einem Neustart des Clients korrekt. Wenn Sie System Manager-Agenten installieren, fordert Clientsetup die Clients zum Neustart auf, wenn die Installation abgeschlossen ist.

System Manager für Server werden nur auf einem Server-Betriebssystem installiert und der Systemverwalter wird nur auf einem Client-Betriebssystem installiert. Wenn Sie eine Serverkonfiguration an ein Clientbetriebssystem oder eine Clientkonfiguration an ein Serverbetriebssystem verteilen, meldet das Clientsetup die erfolgreiche Durchführung der Operation und außer den von Ihnen gewählten System Manager-Komponenten werden alle anderen Komponenten installiert.

Weitere Informationen zur Verteilung von Client Setup-Konfigurationen finden Sie im *Installations- und Verteilungshandbuch*.

Arbeiten mit Server Manager- und Systemverwalter-Clients

Nachdem Sie System Manager-Clients auf dem Netzwerk installiert haben, können Sie sie über die Management Suite-Konsole verwalten. Durch Klicken auf **Extras | Systemverwalteradministration** wird das Fenster "Systemverwalteradministration" angezeigt, in dem Sie Server Manager- und System Manager-Clients verwalten können.

Sie können überprüfen, ob der Systemverwalteragent auf einem Client installiert ist, indem Sie einen Client auswählen und in dessen Kontextmenü auf **Eigenschaften** und dann auf die Registerkarte **Agenten** klicken.

Wenn Sie einen Systemverwalter-Client in der Netzwerkansicht der Konsole auswählen, können Sie im Kontextmenü dieses Client auf **Systemverwalter** klicken, um ein separates Fenster anzuzeigen, in dem nur der von Ihnen ausgewählte Client verwaltet wird.

Ausführen des Client-Setup-Assistenten

Im Client-Setup-Assistent (**Extras | Clientsetup**) passen Sie Clientkonfigurationen Ihren Bedürfnissen an. In diesem Assistenten können Sie die zu installierenden Komponenten und die Optionen für diese Komponenten angeben. Sie können so viele Clientkonfigurationen erstellen wie Sie möchten. Es kann jedoch nur eine Standardkonfiguration geben.

Hinweis: Berücksichtigen Sie bei der Verwendung des Client-Setup-Assistenten zum Erstellen einer neuen Standard-Clientkonfiguration, dass alle Clients, die sich beim Core Server mit Anmeldeskripts anmelden bei der nächsten Anmeldung automatisch mit den neuen Standardkonfigurationseinstellungen rekonfiguriert werden, auch wenn ihre aktuellen Einstellungen den neuen Standardeinstellungen entsprechen.

Änderungen an der Standard-Clientkonfiguration auf dem Core Server werden nicht automatisch an andere aktuell installierte Clientverteilungsdienst-Center weitergegeben. Sie müssen die Clientverteilungsdienst-Center neu installieren, um ihre Standardeinstellungen entsprechend den Einstellungen auf dem Core Server zu aktualisieren.

In den folgenden Abschnitten werden die Seiten des Client-Setup-Assistenten beschrieben.

Informationen zum Client-Setup-Assistenten: Seite "Komponenten installieren"

Der Client-Setup-Assistent: Die Seite "Komponenten installieren" enthält die folgenden Funktionen:

- **Konfigurationsname**: Der Name der Datei mit den Konfigurationseinstellungen. Dieser Name wird auf der Symbolschaltfläche "Einstellungsdatei" im Fenster "Client Setup" angezeigt.
- **Application Healing**: Unterstützt die Ausführung von konfigurierten Anwendungen auf den Clients. Schützen Sie damit kritische oder häufig verwendete Anwendungen.
- **Application Policy Management**: Eine Reihe von Anwendungen werden automatisch auf Clientgruppen installiert. Verwalten Sie damit Gruppen von Clients, die die gleiche Software benötigen.
- **Bandbreitenerkennung**: Ermöglicht die Bandbreitenerkennung zwischen Clients und Core Server. Sie können Management Suite-Aktionen, wie z. B. Software Distribution, von der verfügbaren Bandbreite abhängig machen. Verwenden Sie diese Option, wenn Fernclients oder Clients vorhanden sind, die über eine langsame Verbindung eine Netzwerkverbindung herstellen.
- **Common Base Agent**: Der CBA, der die Kommunikationsbasis zwischen den Clients und dem Core Server darstellt, wird installiert. Die meisten Komponenten benötigen den Common Base Agent.
- **Benutzerdefinierte Datenformulare**: Den Benutzern wird ein Formular zum Ausfüllen angezeigt. Sie können die von Benutzern eingegebenen Daten in der Core-Datenbank abfragen. So können Sie benutzerdefinierte Daten von Benutzern direkt abrufen.
- **Migrationstasks aktivieren**: Die für OSD und die Profilmigration erforderlichen Komponenten werden ausgewählt: Bandbreitenerkennung, Common Base Agent und Enhanced Software Distribution.

- **Enhanced Software Distribution**: Die Installation von Softwareanwendungen und die Verteilung von Dateien an Clients werden automatisiert. So können Sie Anwendungen gleichzeitig auf mehreren Clients installieren oder Dateien oder Treiber auf mehreren Clients aktualisieren.
- **Inventarscanner**: Er sammelt Software- und Hardware-Daten für Clients, die Sie über Datenbankabfragen anzeigen können. Halten Sie so detaillierte Inventardaten über alle Clients fest.
- **Local Scheduler**: So können "Application Policy Management" und "Taskfertigstellen" auf Clients zu bestimmten Zeiten ausgeführt werden. Verwenden Sie diese Funktion, wenn Sie "Application Policy Management" oder "Taskfertigstellen" nicht bei der Anmeldung ausführen möchten, oder wenn die Agenten häufiger/weniger häufig ausgeführt werden sollen.
- **Fernsteuerung**: Damit können Sie über das Netzwerk die Kontrolle über einen Client oder Server übernehmen. Damit wird die Zeit, die für die Lösung von Kundenproblemen von einem zentralisierten Helpdesk aus benötigt wird, minimiert. Sie können mit dieser Funktion Fernmanagement von Clients über das LAN/WAN anbieten.
- **Softwarelizenzüberwachung**: Diese Funktion überwacht die Verwendung von Softwarelizenzen und erstellt dazu Berichte.
- **Targeted Multicasting**: Fügt Targeted Multicast-Unterstützung für ESWD, Application Policy Management, Application Healing, OSD usw. hinzu.
- **Taskfertigstellen**: Überprüft den Core Server, ob Tasks vorhanden sind, die der Client ausführen muss. Verwenden Sie diese Funktion für Clients, mit denen nur hin und wieder eine Verbindung besteht (z. B. mobile Benutzer), um sicherzustellen, dass sie geplante Tasks erhalten.

Wenn Sie LANDesk Server Manager oder LANDesk-Systemverwalter installieren (beide sind unabhängig voneinander verfügbar), werden möglicherweise diese zusätzlichen Optionen angezeigt:

Zusätzliche Serverkonfigurationsoptionen

- **Systemverwalter (Server):** Installiert die Server Manager-Agenten auf dem Server, sodass Sie die Echtzeit-Statusüberwachung, die Alarmfunktion und die Sammlung von historischen Daten möglich ist.
- **Fernsteuerung für Server:** Installiert eine spezielle Fernsteuerungsversion auf Anwendungsebene für erhöhte Zuverlässigkeit. Durch Ausführen der Fernsteuerung auf Anwendungsebene anstatt auf Treiberebene sind die Server weniger anfällig für Fernsteuerungsprobleme.

Zusätzliche Clientkonfigurationsoptionen

- **Systemverwalter:** Installiert die Systemverwalteragenten auf Clients, sodass die Echtzeit-Statusüberwachung, die Alarmfunktion usw. möglich ist.
- **Mobile Manager-Unterstützung:** Installiert den Systemverwalteragenten für mobile Clients.

Verteilen der Fernsteuerung

Bei der Verteilung der Fernsteuerung müssen Sie sich entscheiden, welches Sicherheitsmodell Sie verwenden möchten. Die folgenden Möglichkeiten stehen Ihnen zur Verfügung:

- **Lokale Vorlage:** Als das einfachste Sicherheitsmodell verwendet die lokale Vorlage jede beliebige Fernsteuerungseinstellung, die auf dem Client angegeben ist. Dieses Modell verlangt keine zusätzliche Authentifizierung oder Gruppenmitgliedschaft.
- **Windows NT-Sicherheit/lokale Vorlage:** Dieses Sicherheitsmodell verwendet eine Windows NT-Fernsteuerungsoperatoren-Gruppe. Die Mitglieder dieser Gruppe sind berechtigt, Clients fernzusteuern. Berechtigte Benutzer verwenden trotzdem die Fernsteuerungseinstellungen des Clients, wie zum Beispiel "Berechtigung erforderlich".
- **Zertifikatbasiert/lokale Vorlage:** Diese Option bietet die höchste Sicherheit und ist in der Management Suite 8 neu enthalten. Sie wird auch sichere Fernsteuerung nach Bedarf genannt und wird im nächsten Abschnitt beschrieben.

Warnung: Windows XP-Clients müssen die Internet Connection Firewall für die Fernsteuerung deaktivieren, damit sie funktionieren.
Wenn Clients die Windows XP Internet Connection Firewall aktivieren, ist keine Fernsteuerung möglich.

Informationen zur sicheren Fernsteuerung nach Bedarf

LANDesk Management Suite 8 führt eine neue sichere Fernsteuerung nach Bedarf ein (zertifikatsbasiert/lokale Vorlage), die Sie verwenden können. Diese neue Fernsteuerung hat sich im Vergleich zur Vorversion wie folgt verbessert:

- Fernkonsolen authentifizieren sich beim Core Server.
- Der Fernsteuerungsagent auf einem Client wird nach Bedarf geladen, sobald eine Fernsteuerungssitzung vom Core genehmigt wurde.
- Die gesamte Fernsteuerungsauthentifizierung und der Verkehr wird über eine SSL-Verbindung verschlüsselt.
- Nachdem die Fernsteuerung auf einem Client abgeschlossen ist, wird der Fernsteuerungsagent beendet.

Der Kommunikationsfluss der Fernsteuerung sieht wie folgt aus:

1. Die Management Suite-Konsole bittet den Core Server um Erlaubnis, den angegebenen Client fernsteuern zu dürfen.
2. Wenn die Konsole/der Benutzer zur Fernsteuerung des Client autorisiert ist, weist der Core Server den Client an, den Fernsteuerungsagenten mit einer zufällig generierten Reihe von Berechtigungsnachweisen für die Authentifizierung zu laden.
3. Der Core Server leitet die Berechtigungsnachweise für die Authentifizierung an die Konsole weiter.
4. Die Konsole authentifiziert sich beim Client mit den Berechtigungsnachweisen, und die Fernsteuerung beginnt.

Warnung: Die sichere Fernsteuerung nach Bedarf benötigt den Core Server
Bei der sicheren Fernsteuerung nach Bedarf muss der Core Server verfügbar sein, sonst können die Konsolen die Clients nicht fernsteuern Für die sichere Fernsteuerung nach Bedarf muss der Core Server funktionieren.

Verwenden der Windows NT-Sicherheit/lokale Vorlage mit Windows XP-Clients

Damit die Windows NT-Sicherheit/Authentifizierung über lokale Vorlage bei Windows XP-Clients funktioniert, müssen Sie Clients so konfigurieren, dass das Standard-Windows XP-Freigabe- und Sicherheitsmodell für lokale Konten verwendet wird (lokale Benutzer authentifizieren sich als sie selbst). Wenn Sie dies nicht tun, funktioniert die standardmäßige Authentifizierung, die nur auf Gäste beschränkt ist, nicht zusammen mit der Windows NT-Sicherheit der Fernsteuerung.

So legen Sie das Standard-Windows XP-Sicherheitsmodell fest

1. Klicken Sie am Windows XP-Client auf **Start | Systemsteuerung**.
2. Klicken Sie im Applet **Verwaltung, Lokale Sicherheitsrichtlinie** auf **Sicherheitsoptionen > Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten** und wählen Sie die Einstellung **Klassisch - lokale Benutzer authentifizieren sich als sie selbst**.

Informationen zum Client-Setup-Assistenten: Seite "Authentifizierung"

Clientsetup: Die Seite "Authentifizierung" wird immer angezeigt. Wenn Sie auf der Seite "Komponenten installieren" nicht die Funktion "Fernsteuerung" aktiviert haben, sind die Vorlagenoptionen nicht verfügbar. Die Seite enthält die folgenden Funktionen:

- **Vertrauenswürdige Zertifikate:**Wählen Sie die Core Server-Zertifikate aus, die von den Clients akzeptiert werden sollen. Clients kommunizieren nur mit Cores und Konsolen, für die sie Zertifikate haben. Weitere Informationen zu Zertifikaten und dem Kopieren von Zertifikaten von anderen Core Servern, um sie hier auswählen zu können, finden Sie unter "Client-Agent-Sicherheit und vertrauenswürdige Zertifikate" weiter oben in diesem Kapitel.
- **Lokale Vorlage:** Verwendet nur die einfachen Berechtigungen des lokalen Client und das Authentifizierungsset der Seite "Fernsteuerungseinstellungen" in diesem Assistenten.
- **Windows NT-Sicherheit/lokale Vorlage:**Nur Mitglieder der Fernsteuerungsoperatoren-Gruppe dürfen Fernsteuerungsverbindungen von der Konsole zu den Fernclients initiieren. Genehmigte Benutzer müssen trotzdem den Berechtigungssatz von der Seite "Fernsteuerungseinstellungen" in diesem Assistenten verwenden.
  Da es sich bei der Gruppe "Fernsteuerungsoperatoren" um eine lokale Gruppe handelt, besitzt jeder Client eine eigene Kopie der Gruppe. Um nicht jede Fernsteuerungsoperatoren-Gruppe einzeln verwalten zu müssen, fügen Sie zu jeder lokalen Gruppe eine globale Gruppe (auf Domänenebene) hinzu. Berechtigte Benutzer verwenden trotzdem die Fernsteuerungseinstellungen des Clients, wie zum Beispiel "Berechtigung erforderlich".

- **Zertifikatbasiert/lokale Vorlage:**Die Kommunikation zwischen der Konsole und den Fernclients wird über den Core Server authentifiziert; nur Konsolen mit Authentifizierung vom gleichen Core Server können Fernsteuerungsfunktionen für die entsprechenden Clients verwenden. Wählen Sie die Zertifikate aus, die Sie in der Liste "Vertrauenswürdige Zertifikate" zulassen möchten. Genehmigte Benutzer müssen trotzdem den Berechtigungssatz von der Seite "Fernsteuerungseinstellungen" in diesem Assistenten verwenden. Diese Option wird auch "sichere Fernsteuerung nach Bedarf" genannt, wie bereits in diesem Kapitel beschrieben.

Hinzufügen von Benutzern zur Fernsteuerungsoperatoren-Gruppe

Wenn Sie als Sicherheitsmodell **Windows NT-Sicherheit/lokale Vorlage** gewählt haben, führt das Dialogfeld "Zur Fernsteuerungsoperatoren-Gruppe hinzufügen" die Benutzer für die Konsole oder für die ausgewählte Windows NT-Domäne auf. Die hier ausgewählten Benutzer, haben Fernsteuerungszugriff auf die Clients, die die Einstellungen empfangen, die Sie in der Datei mit den Konfigurationseinstellungen festgelegt haben.

Dieses Dialogfeld können Sie nur im Client-Setup-Assistenten aus dem Fenster "Clientsetup" öffnen.

So wählen Sie von einem vorhandenen Server oder einer Domäne

1. Wählen Sie im Kombinationsfeld **Namen auflisten aus** entweder den Core Server-Namen oder eine Windows NT-Domäne, die Benutzerkonten enthält, aus.
2. Wählen Sie im Feld **Namen** einen oder mehrere Benutzer aus und klicken Sie anschließend auf **Einfügen**, um sie zur Liste **Eingefügte Namen** hinzuzufügen.
3. Klicken Sie auf **OK**, um die ausgewählten Namen auf jedem Client, der die Konfigurationseinstellungen empfängt, zur Fernsteuerungsoperatoren-Gruppe hinzuzufügen.

So geben Sie Namen manuell ein

Sie können Namen manuell eingeben, indem Sie in die Liste "Eingefügte Namen" klicken und Namen in einem der folgenden Formate eingeben. Zur Trennung von Namen verwenden Sie Strichpunkte.

- **DOMAIN\username**, wobei DOMAIN der Name einer Domäne ist, auf die der Ziel-Client zugreifen kann.
- **MACHINE\username**, wobei MACHINE der Name eines Client ist, der sich in derselben Domäne wie der Ziel-Client befindet.
- **DOMAIN\groupname**, wobei DOMAIN der Name einer Domäne ist, auf die der Ziel-Client zugreifen kann, und groupname der Name einer Verwaltungsgruppe in dieser Domäne.
- **MACHINE\groupname**, wobei MACHINE der Name eines Client in derselben Domäne ist, in der sich der verwaltete Knoten befindet, und groupname der Name einer Verwaltungsgruppe auf diesem Client.

Wenn Sie keinen Domänen- oder Clientnamen angeben, wird angenommen, dass der angegebene Benutzer oder die Gruppe zum lokalen Client gehört.

Klicken Sie auf **OK**, um die Namen zur Fernsteuerungsoperatoren-Gruppe auf dem Ziel-Client hinzuzufügen.

Informationen zum Client-Setup-Assistenten: Fernsteuerung - Einstellungsseite

Clientsetup: Die Seite "Fernsteuerung" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" die Fernsteuerung aktiviert haben. Die Seite enthält die folgenden Funktionen:

- **Berechtigung erforderlich:** Der Konsolenbenutzer muss eine Berechtigung vom Client erhalten, ehe ihm ein Fernzugriff gewährt wird.
- **Nach allen zulässigen Berechtigungen gleichzeitig fragen:** Fragt den Benutzer einmal nach einer Sitzungsberechtigung. Bei der Funktion Berechtigung erforderlich muss der Benutzer für Fernsteuerung, Chat, Dateiübertragung usw. einzeln Berechtigungen vorweisen. Diese Option gewährt dem Benutzer die Berechtigung für alle mit der Fernsteuerung zusammenhängenden Optionen während einer Sitzung.
- **Clientmeldungen anzeigen:** Agentfehlermeldungen werden angezeigt. Wenn Sie diese Funktion nicht wählen, werden Fehler im Ereignisprotokoll festgehalten.
- **Signalton, wenn Fernsteuerung eingerichtet ist:** Solange der Client ferngesteuert wird, ertönt alle zehn Sekunden ein Alarm.
- **Clients dürfen Einstellungen ändern:** Das Symbol "Fernsteuerungseinstellungen" wird zur Programmgruppe des Client unter Start | Programme | LANDesk Management hinzugefügt. Clients können über dieses Programm ihre Fernsteuerungsoptionen anpassen.
- **Daten komprimieren:** Bewirkt eine drastische Reduzierung des Bedarfs an Netzwerkbandbreite für eine Fernsteuerungssitzung.
- **Unverankertes Desktop-Symbol (Fernsteuerungsanzeige):** Das Symbol "Fernsteuerungsagent" wird ständig auf dem Clientbildschirm angezeigt oder nur, wenn er ferngesteuert wird. Wenn der Client von der Konsole gesteuert wird, ändert sich das Symbol in eine Lupe, und die Titelleiste des Symbols wird rot.
- **Taskleistensymbol (Fernsteuerungsanzeige):** Fügt das Symbol "Fernsteuerungsagent" in die Taskleiste ein. Auch bei dieser Funktion kann das Symbol ständig angezeigt werden oder nur, wenn der Client ferngesteuert wird.

Berechtigung erforderlich, wenn ein Benutzer angemeldet ist

Wenn Sie die Einstellung "Fernsteuerungsberechtigung erforderlich" im Clientsetup oder der Datei EDITINI aktivieren, können Sie keinen anderen Windows NT- oder Windows 2000-/20003-/XP-Computer fernsteuern, solange der Benutzer es nicht zulässt. Wenn an dem Client, den Sie fernsteuern möchten, niemand angemeldet ist, und die Einstellung "Berechtigung erforderlich" aktiviert ist, kann Ihnen niemand diese Berechtigung erteilen.

Für dieses Problem gibt es eine weitere Einstellungsart "Berechtigung erforderlich", die eine Berechtigung nur dann erforderlich macht, wenn jemand angemeldet ist. Für diese Einstellung müssen Sie die Datei NTSTACFG.INI im Verzeichnis LDLOGON manuell ändern und anschließend WSCFG32.EXE auf den Clients erneut ausführen, die über die neue Einstellung "Berechtigung erforderlich" verfügen sollen.

Um die Einstellung in der Datei NTSTACFG.INI zu ändern, öffnen Sie sie und suchen Sie nach dem Eintrag "Berechtigung erforderlich"; ändern Sie in diesem den aktuellen Wert (0 oder 1) auf 2.

Informationen zum Client-Setup-Assistenten: Seite "Fernsteuerung"

Clientsetup: Die Seite "Fernsteuerung" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" die Fernsteuerung aktiviert haben. Die Seite enthält die folgenden Funktionen:

- **Fernsteuerung:** Erteilt die Berechtigung, den Client zu steuern.
- **Neu starten:** Erteilt die Berechtigung, den Client neu zu starten.
- **Chat:** Erteilt die Berechtigung zur Eröffnung einer Chat-Sitzung mit dem Client.
- **Dateiübertragung:** Erteilt die Berechtigung, Dateien an und von den lokalen Laufwerken des Client zu übertragen.
- **Fernausführung:** Erteilt die Berechtigung, Programme auf dem Client auszuführen.

Sie können außerdem Mitglieder zur Fernsteuerungsoperatoren-Gruppe auf Ziel-Windows NT- oder Windows 2000-/2003-Clients hinzufügen. Diese Benutzer können über die Konsole die Ziel-Clients fernsteuern, wenn Sie die Option **Windows NT-Sicherheit/lokale Vorlage** auf der Seite "Authentifizierung" auswählen.

Klicken Sie auf **Hinzufügen**, um ein Dialogfeld zu öffnen, in dem Sie Mitglieder für die Fernsteuerungsoperatoren-Gruppe auf Windows NT-/2000-/2003-Clients angeben.

Um einen Namen aus der Liste zu entfernen, markieren Sie ihn und klicken Sie auf **Entfernen**.

Verteilen des Inventars

Informationen zum Client-Setup-Assistenten: Seite "Inventarscanner"

Clientsetup: Die Seite "Inventarscanner" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" den Inventarscanner aktiviert haben. Die Seite enthält die folgenden Funktionen:

- **Manuelle Aktualisierung:** Die Softwareliste, die verwendet wird, um Titel beim Durchführen von Softwarescans auszuschließen, wird auf jeden Fernclient heruntergeladen. Jedes Mal wenn die Softwareliste auf der Konsole geändert wird, müssen Sie sie manuell an die Fernclients senden.

- **Automatische Aktualisierung:** Die Fernclients lesen die Softwareliste während der Softwarescans vom Core Server. Wenn Sie diese Option wählen, muss jeder Client über ein Laufwerk verfügen, das dem Verzeichnis LDLOGON auf dem Core Server zugewiesen ist, damit er auf die Softwareliste zugreifen kann. Änderungen an der Softwareliste stehen den Clients sofort zur Verfügung.
    - **Aktualisierung mit HTTP:** Ab Management Suite 8 kann der Inventarscanner HTTP für LDAPPL3.INI-Dateiübertragungen verwenden. Dadurch unterstützt der Scanner Targeted Multicast-Funktionen wie Polite-Bandbreite und Peer Download. Ein Peer Download ermöglicht Clients, die LDAPPL3.INI-Updates benötigen, auf dem Core Server nach dem Datum der neuesten Version zu suchen. Anschließend stellen die Clients eine Verbindung zu Peers im Subnetz her, um zu ermitteln, ob ein Peer das Update in seinem Multicast-Cache hat. Verfügt ein Peer über das Update, erfolgt der Dateitransfer im lokalen Subnetz ohne Erzeugung von Netzwerkverkehr über Router oder WAN-Verbindungen.
- **Inventarscanner starten in:** Mit der neben dieser Option angezeigten Dropdown-Liste können Sie eine der folgenden Optionen auswählen: **In Startgruppe**, **Zwischen Stunden** und **Manuell von Client**. Wenn Sie den Inventarscanner von der Startgruppe aus starten, wird der Scanner jedes Mal ausgeführt, sobald sich der Benutzer anmeldet. Benutzer, die den Scanner manuell ausführen möchten, können den Scanner von **Start | Programme | LANDesk Management | Inventarscan** aus starten.

Verwenden der Inventarscanner-Option "Zwischen Stunden"

Wenn Sie die Inventarscanner-Option **Zwischen Stunden** auswählen, können Sie unter Verwendung des 24-Stunden-Formats einen Stundenbereich angeben. Meldet sich ein Client während des angegebenen Zeitraums an, so wird automatisch der Inventarscanner ausgeführt. Wenn der Client bereits angemeldet ist, wird der Scan zur angegebenen Stundenzeit automatisch gestartet. Diese Option ist nützlich, wenn Sie Inventarscans auf Clients zeitlich versetzt ausführen möchten, um zu verhindern, dass alle Scans gleichzeitig gesendet werden.

Informationen zum Client-Setup-Assistenten: Seite "Inventarscanner" (Bereich)

Um die rollenbasierte Administration zu implementieren, verwendet die Management Suite Gerätebereiche, die steuern, welche Clients ein Benutzer sehen und verwalten kann. Ein Administrator erstellt Bereiche und weist sie Benutzern zu. Bereiche können basieren auf:

- **Datenbankabfragen: Beschränken den Zugriff auf die Clients, die einer benutzerdefinierten Abfragesuche entsprechen**.
- **LDAP-Verzeichnisse:** Wenn Sie ein Active Directory oder eine Netware eDirectory LDAP-kompatible Struktur haben, können Sie diese Verzeichnispfade verwenden, um Bereiche zu definieren.

- **Benutzerdefinierte Verzeichnisse:** Wenn Sie weder über eine Active Directory- noch über eine NetWare eDirectory LDAP-kompatible Struktur verfügen oder einen benutzerdefinierten Verzeichnispfad verwenden möchten, geben Sie diesen Pfad auf dieser Seite des Assistenten ein. Wenn ein Client konfiguriert wird, bestimmt der Pfad, den Sie hier eingeben, den Computerstandort-Attributwert des Clients.

Wenn der Inventarscanner auf einem Client ausgeführt wird, zeichnet er das Computerstandort-Attribut des Client auf. Wenn Sie in der Client-Setup-Konfiguration des Client einen benutzerdefinierten Verzeichnispfad eingegeben haben, zeichnet der Scanner diesen Pfad als Standort auf. Wenn Sie keinen benutzerdefinierten Verzeichnispfad eingegeben haben, versucht der Scanner, das Inventarattribut mit dem Active Directory- oder dem NetWare eDirectory-Standort einzutragen. Wenn weder ein benutzerdefiniertes Verzeichnis noch ein LDAP-kompatibles Verzeichnis gefunden wird, ist das Computerstandort-Attribut nicht definiert. Der Client kann jedoch trotzdem in Abfrage-basierten Bereichen erfasst werden.

Die Bereichsseite des Client-Setup-Assistenten verwendet ein Pfadformat, das einem Dateipfad ähnelt; die einzelnen Segmente werden jedoch durch Schrägstriche getrennt. Wenn Sie Bereiche verwenden möchten, die auf Verzeichnissen basieren, müssen Sie sich die Kategorien für die zu verwaltenden Knoten überlegen. Sie können beispielsweise die geographische Lage, Büros oder Organisationseinheiten wählen.

Verzeichnisstandortpfade, die Sie hier als Teil einer Clientkonfiguration eingeben, werden der Registrierung des Client hinzugefügt unter:

```
HKLM\Software\Intel\LANDesk\Inventory\ComputerLocation
```

Weitere Informationen finden Sie unter "Rollenbasierte Administration" in Kapitel 1.

Verteilen von Application Healing

Der Application Healing-Agent repariert automatisch Anwendungen auf dem Client, die nicht mehr ausgeführt werden, weil Dateien versehentlich gelöscht oder beschädigt wurden. Mit Application Healing können Sie Management Suite so konfigurieren, dass die von Ihnen angegebenen Anwendungen repariert werden.

Application Healing erfordert die Komponenten Common Base Agent und Enhanced Software Distribution.

Wenn Sie die Agenten Application Policy Management oder Application Healing auswählen, wird auch die Seite "Clientstatus-TCP-Port" angezeigt. Hier wird der Port angegeben, den Clients zur Übermittlung von Statusinformationen an den Core Server benutzen. Standardmäßig wird Port 12175 verwendet.

Informationen zum Client-Setup-Assistenten: Seite "Application Healing"

Client-Setup: Die Seite "Application Healing" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" "Application Healing" aktiviert haben. Die Seite enthält die folgenden Funktionen:

- **Application Healing deaktivieren (Alarme aktiviert):** Aktiviert Application Healing AMS-Alarme, deaktiviert jedoch den Healing-Vorgang. Mit dieser Funktion können Sie herausfinden, welche Anwendungen auf Ihren Clients nicht richtig laufen. Wenn eine Anwendung fehlschlägt, werden von Ihnen konfigurierte AMS-Alarme ausgelöst; weiter geschieht auf dem Client nichts.
- **Dialogtimeout:** Gibt in Sekunden an, wie lange der Clientdialog auf eine Antwort warten soll, ehe eine defekte Anwendung repariert wird. Dieser Wert ist sinnvoll, wenn niemand am Client ist und Sie eine Anwendung reparieren möchten.
- **Healing-Abstand:** Gibt in Sekunden an, wie lange der Application Healing-Agent mit der erneuten Reparatur einer Anwendung warten soll, nachdem bereits eine Reparatur versucht wurde. Dieser Wert ist sinnvoll, wenn Application Healing aus einem unbekannten Grund eine Anwendung nicht reparieren kann. Application Healing soll nicht in einem Reparatur-Loop auf einem Client hängenbleiben.
- **Kein Feedback für Benutzer anzeigen**: Wenn Sie diese Option wählen, wird das Paket im Hintergrund installiert, wenn es nicht ursprünglich mit Benutzerschnittstellen-Anpassungen erstellt wurde.
- **Alternativer Paketspeicherort zulässig:** Wenn Sie diese Option wählen, haben Sie die Möglichkeit, einen alternativen Reparaturpaket-Speicherort für erforderliche Reparaturen anzugeben. Alternative Paketspeicherorte sind für mobile Benutzer sinnvoll, die nicht mit dem Netzwerk verbunden sind und eine CD mit Reparaturpaketen verwenden.
- **Benutzer darf Reparatur verzögern:** Wenn diese Option ausgewählt ist, sind Benutzer berechtigt, Reparaturen zu verzögern.
- **Benutzer darf abbrechen:** Wenn diese Option ausgewählt ist, sind Benutzer berechtigt, aktive Reparaturvorgänge abzubrechen. Diese Option ist standardmäßig aktiviert.
- **Hintergrundbildschirm anzeigen:** Wenn diese Option ausgewählt ist, verwendet der Application Healing-Agent während des Reparaturvorgangs einen blauen Splash-Bildschirm.

Informationen zum Client-Setup-Assistenten: Seite "Anwendungsreparaturlisten (ARL)"

Client-Setup: Die Seite "Anwendungsreparaturlisten (ARL)" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" "Application Healing" aktiviert haben. Die Seite enthält die folgenden Funktionen:

- **ARLs zum Senden mit Client auswählen:** Wenn Sie Application Healing bereits konfiguriert haben, um Anwendungen wie im *Benutzerhandbuch* beschrieben zu reparieren, verfügen Sie über ARL-Dateien, die Sie zusammen mit Agenten an Clients verteilen können. Wenn Sie Application Healing noch nicht konfiguriert haben, können Sie die Agenten ohne die ARL-Dateien verteilen. Application Healing wird erst aktiviert, wenn die Clients über den Agenten und die ARL-Dateien verfügen.

Verteilen von Application Policy Management

Der Application Policy Management-(APM-)Agent ermöglicht die automatische Installation bestimmter Anwendungsgruppen auf Gruppen von Clients. Verwenden Sie diesen Agenten, um Gruppen von Clients zu verwalten, die die gleiche Software benötigen. APM erfordert die Agenten Common Base Agent und Enhanced Software Distribution.

Damit Clients Richtlinien empfangen können, die über Active Directory- oder NetWare-Verzeichnisdienste angegeben werden, muss für sie die Anmeldung beim Verzeichnis konfiguriert werden. Das bedeutet, dass die richtige Clientsoftware installiert sein muss. Außerdem müssen sich die Clients beim richtigen Verzeichnis anmelden, damit ihr eindeutiger, definierter Name dem Namen entspricht, der über Directory Manager und Application Policy Manager angegeben wurde.

Windows 95/98-Clients müssen so konfiguriert sein, dass ihre Anmeldung bei der Domäne erfolgt, die Active Directory enthält. Active Directory wird von Windows NT und Windows 95/98 nicht unterstützt. Sie müssen auf den Clients, die sich bei einem Verzeichnis anmelden und Application Policy Management erfordern, Active Directory-Unterstützung installieren. Zum Zeitpunkt der Veröffentlichung waren unter folgender Adresse weitere Informationen zur Active Directory-Clientunterstützung erhältlich:

http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp

Informationen zum Client-Setup-Assistenten: Seite "Application Policy Management"

Client-Setup: Die Seite "Application Policy Management" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" die Option "Application Policy Management" aktiviert haben. Auf dieser Seite können Sie die Details für jede Option konfigurieren, indem Sie auf die Schaltfläche **Konfigurieren** klicken.

Die Seite enthält die folgenden Funktionen:

- **Application Policy Management-Verknüpfung zur LANDesk Management-Startmenügruppe hinzufügen:** Erstellt eine LANDesk Management Suite-Programmgruppe, mit der Clients die APM-Agentenbenutzerschnittstelle manuell ausführen können. Der Agent sollte nur Pull-Tasks, die sich aktuell im Cache befinden, ausführen.
- **APM-Client bei jeder Benutzeranmeldung starten:** Der APM-Agent wird ausgeführt, wenn sich Benutzer anmelden. Der Agent sucht nach Richtlinien und schließt sich nach Abschluss der Suche automatisch.
- **APM-Client in festgelegten Zeitabständen starten (Local Scheduler für Clients erforderlich):** Der Client-Agent wird nur zu bestimmten Zeiten ausgeführt.

Informationen zum Client-Setup-Assistenten: Dialogfeld "Application Policy Management-Optionen"

Das Dialogfeld "Application Policy Management-Optionen" wird angezeigt, wenn Sie auf der Seite "Application Policy Management-Assistent" auf die Schaltfläche **Konfigurieren** klicken.

Die Seite enthält die folgenden Funktionen:

- **APM-Client im Hintergrund ausführen:** APM wird ausgeführt, ohne dass die Clientschnittstelle angezeigt wird.
- **Erforderliche Richtlinien ausführen und übrige im Cache ablegen:** Die erforderlichen Richtlinien werden ausgeführt. Bevorzugte und optionale Richtlinien werden lokal im Cache abgelegt, falls die Clients diese Richtlinien später installieren möchten.
- **Nur Richtlinien aus lokalem Cache des Client ausführen:** Nur Richtlinien aus dem Cache werden ausgeführt. Die Clients initiieren keinen Netzwerkverkehr.
- **Clienttimeout:** Verzögerungstimeout in Sekunden.
- **Alle Netzwerkverbindungen zulassen:** Die Richtlinie wird unabhängig von der Verbindungsart der Clients ausgeführt. Wenn alle Ihre Clients über einen Hochgeschwindigkeits-Netzwerkzugriff auf den Paketserver verfügen, ist diese Option empfehlenswert.
- **Alle Nicht-RAS-Netzwerkverbindungen zulassen:** Die Richtlinie wird ausgeführt, wenn die Verbindung des Client zum Paketserver mindestens WAN-Geschwindigkeit, aber weniger als LAN-Geschwindigkeit hat. Die LAN-Geschwindigkeit ist standardmäßig als 262.144 Bit/s definiert.
- **Nur Hochgeschwindigkeitsverbindung zulassen:** Die Richtlinie wird ausgeführt, wenn die Verbindung des Client zum Paketserver die LAN-Geschwindigkeitseinstellung (standardmäßig 262.144 Bit/s) übertrifft..

Informationen zum Client-Setup-Assistenten: Dialogfeld "Application Policy Management-Optionen" (angegebene Intervalle)

Das Dialogfeld "Application Policy Management-Optionen" wird angezeigt, wenn Sie auf der Seite "Application Policy Management-Assistent" auf die Schaltfläche **Konfigurieren** klicken.

Sie können außerdem angeben, dass der Application Policy Management-Agent periodisch oder nur in bestimmten Zeiträumen/Tagen/Wochen/Monaten ausgeführt werden soll. Der Agent wird einmal in dem von Ihnen angegebenen **Ausführungsintervall** ausgeführt.

Die Seite enthält die folgenden Funktionen:

- **APM-Client im Hintergrund ausführen:** APM wird ausgeführt, ohne dass die Clientschnittstelle angezeigt wird.
- **Erforderliche Richtlinien ausführen und übrige im Cache ablegen:** Die erforderlichen Richtlinien werden ausgeführt. Bevorzugte und optionale Richtlinien werden lokal im Cache abgelegt, falls die Clients diese Richtlinien später installieren möchten.

- **Nur Richtlinien aus lokalem Cache des Client ausführen:** Nur Richtlinien aus dem Cache werden ausgeführt. Die Clients initiieren keinen Netzwerkverkehr.
- **APM-Client periodisch ausführen:** Aktivieren Sie diese Option und wählen Sie ein **Ausführungsintervall** aus dem Listenfeld. Der Agent wird einmal in dem von Ihnen angegebenen Intervall ausgeführt. Wenn Sie diese Option wählen, klicken Sie auf die Schaltfläche **Zeitfilter** und richten Sie die Intervalldetails ein. Der Benutzer muss sich anmelden, damit der Agent ausgeführt wird.
- **Alle Netzwerkverbindungen zulassen:** Die Richtlinie wird unabhängig von der Verbindungsart ausgeführt. Wenn alle Ihre Clients über einen Hochgeschwindigkeits-Netzwerkzugriff auf den Paketserver verfügen, ist diese Option empfehlenswert.
- **Alle Nicht-RAS-Netzwerkverbindungen zulassen:** Die Richtlinie wird ausgeführt, wenn die Verbindung des Client zum Paketserver mindestens WAN-Geschwindigkeit, aber weniger als LAN-Geschwindigkeit hat. Die LAN-Geschwindigkeit ist standardmäßig als 262.144 Bit/s definiert.
- **Nur Hochgeschwindigkeitsverbindung zulassen:** Die Richtlinie wird ausgeführt, wenn die Verbindung des Client zum Paketserver die LAN-Geschwindigkeitseinstellung (standardmäßig 262.144 Bit/s) übertrifft..

Informationen zum Client-Setup-Assistenten: Dialogfeld "Application Policy Management-Optionen" (Anmeldeoptionen)

Das Dialogfeld "Application Policy Management-Optionen" wird angezeigt, wenn Sie auf der Seite "Application Policy Management-Assistent" auf die Schaltfläche **Konfigurieren** klicken.

Sie können außerdem angeben, dass der Application Policy Management-Agent periodisch oder nur in bestimmten Zeiträumen/Tagen/Wochen/Monaten ausgeführt werden soll. Der Agent wird einmal in dem von Ihnen angegebenen **Ausführungsintervall** ausgeführt.

Die Seite enthält die folgenden Funktionen:

- **APM-Client im Hintergrund ausführen:** APM wird ausgeführt, ohne dass die Clientschnittstelle angezeigt wird.
- **Erforderliche Richtlinien ausführen und übrige im Cache ablegen:** Die erforderlichen Richtlinien werden ausgeführt. Bevorzugte und optionale Richtlinien werden lokal im Cache abgelegt, falls die Clients diese Richtlinien später installieren möchten.
- **Nur Richtlinien aus lokalem Cache des Client ausführen:** Nur Richtlinien aus dem Cache werden ausgeführt. Die Clients initiieren keinen Netzwerkverkehr.
- **APM-Client periodisch ausführen:** Aktivieren Sie diese Option und wählen Sie ein **Ausführungsintervall** aus dem Listenfeld. Der Agent wird einmal in dem von Ihnen angegebenen Intervall ausgeführt. Wenn Sie diese Option wählen, klicken Sie auf die Schaltfläche **Zeitfilter** und richten Sie die Intervalldetails ein. Der Benutzer muss sich anmelden, damit der Agent ausgeführt wird.
- **Clienttimeout:** Verzögerungstimeout in Sekunden.

- **Alle Netzwerkverbindungen zulassen:** Die Richtlinie wird unabhängig von der Verbindungsart der Clients ausgeführt. Wenn alle Ihre Clients über einen Hochgeschwindigkeits-Netzwerkzugriff auf den Paketserver verfügen, ist diese Option empfehlenswert.
- **Alle Nicht-RAS-Netzwerkverbindungen zulassen:** Die Richtlinie wird ausgeführt, wenn die Verbindung des Client zum Paketserver mindestens WAN-Geschwindigkeit, aber weniger als LAN-Geschwindigkeit hat. Die LAN-Geschwindigkeit ist standardmäßig als 262.144 Bit/s definiert.
- **Nur Hochgeschwindigkeitsverbindung zulassen:** Die Richtlinie wird ausgeführt, wenn die Verbindung des Client zum Paketserver die LAN-Geschwindigkeitseinstellung (standardmäßig 262.144 Bit/s) übertrifft..

Informationen zum Client-Setup-Assistenten: Seite "Zeitfilteroptionen"

Das Dialogfeld "Zeitfilteroptionen" steht Ihnen auf den Seiten "Application Policy Management" und "Taskfertigstellen" zur Verfügung. Über Zeitfilter wird der Local Scheduler so konfiguriert, dass die Agenten "Application Policy Management" und "Taskfertigstellen" zu den von Ihnen angegebenen Zeiten gestartet werden. Zeitfilter funktionieren nur auf Clients, auf denen der Local Scheduler installiert ist.

Sie können Zeitfilter verwenden, um Clients so zu konfigurieren, dass die Agenten nach Betriebsschluss oder an den Wochenenden anstatt bei einer Benutzeranmeldung ausgeführt werden.

Das Dialogfeld "Zeitfilteroptionen" bietet Ihnen folgende Optionen:

- **Tageszeitfilter verwenden. Der Task wird erst zu der zwischen den Stundenangaben liegenden Tageszeit ausgeführt.** Wählen Sie Start- und Endzeiten aus.
- **Wochentagfilter verwenden. Der Task wird erst an dem zwischen den angegebenen Tagen liegenden Wochentag ausgeführt.** Wählen Sie Start- und Endtage aus.
- **Monatsdatumfilter verwenden. Der Task wird erst an dem zwischen den Datumsangaben liegenden Tag des Monats ausgeführt.** Wählen Sie ein Start- und Enddatum aus.

Informationen zum Client-Setup-Assistenten: Seite "Bandbreitenerkennung"

Client-Setup: Die Seite "Bandbreitenerkennung" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" "Application Healing" oder "Application Policy Management" aktiviert haben. Die Seite enthält die folgenden Funktionen:

- **Bandbreitenerkennungsmethode wählen:** Wählen Sie aus, ob ICMP oder PDS für die Bandbreitenerkennung verwendet werden soll. ICMP sendet ICMP-Echoanforderungen verschiedener Größe an die Fernclients und verwendet das Antwortverhalten dieser Echoanforderungen bzw. -reaktionen, um die ungefähre Bandbreite zu bestimmen. ICMP unterscheidet auch zwischen LAN (Hochgeschwindigkeits-) und WAN (langsame, jedoch keine Einwahl-) Verbindungen. Nicht alle Router oder Clients unterstützen jedoch ICMP-Echoanforderungen. Wenn das Netzwerk nicht für das Zulassen von ICMP-Echoanforderungen konfiguriert ist, können Sie PDS wählen. Die PDS-Bandbreitentests sind nicht so detailliert, aber sie finden entweder eine LAN- oder RAS-Verbindung (in der Regel Einwahlverbindungen) mit geringer Bandbreite.
- **LAN-Schwellenwert, in Bit/Sekunde:** Der Schwellenwert, der eine Verbindung als WAN und nicht als LAN klassifiziert. Der Standardwert ist 262.144 Bit/s.
- **Dyn. Bandbreitendrosselung aktivieren:** Legt fest, dass der von einem Client erzeugte Netzwerkverkehr Vorrang vor dem durch die Verteilung bedingten Verkehr hat. Diese Option erzwingt zudem, dass die gesamte Datei in den Cache des Clients heruntergeladen wird. Damit wird gleichzeitig die Option für Checkpoint-Neustarts auf Byte-Ebene aktiviert, sodass Downloadvorgänge im Fall einer Unterbrechung an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden,.
  Diese Option ist auch über den Assistenten für das Bereitstellen von Paketen verfügbar. Wenn Sie diese Option in Clientsetup aktivieren, jedoch nicht im Assistenten für das Bereitstellen von Paketen, ist sie auf dem Client weiterhin aktiviert. Wenn Sie diese Option in Clientsetup nicht aktivieren, jedoch im Assistenten für das Bereitstellen von Paketen aktivieren, wird die dynamische Bandbreitendrosselung auf dem Client für dieses Paketskript aktiviert.

Informationen zum Client-Setup-Assistenten: Seite "Clientstatus-TCP-Port"

Clientsetup: Die Seite "Clientstatus-TCP-Port" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" die Option "Application Healing" oder "Application Policy Management" aktiviert haben. Die Seite enthält die folgenden Funktionen:

- **TCP-Port:** Gibt den Port an, den der Agent Application Healing/Application Policy Management zur Kommunikation mit dem Core Server verwendet. Der Standardport ist 12175. Sie müssen sicherstellen, dass der Port in allen Firewalls zwischen den Clients und dem Core Server offen ist. Wenn Sie diesen Port ändern, müssen Sie ihn auch auf dem Core Server ändern. Sie können den Port, den der QIP-Serverdienst verwendet, ändern, indem Sie diesen Registrierungsschlüssel bearbeiten:

  HKLM\Software\Intel\LANDesk\LDWM\QIPSrvr

Informationen zum Starten des APM-Client in festgelegten Zeitabständen

Die Zeitabstände, in denen der Application Policy Management-Client automatisch gestartet wird, werden über zwei Dialogfelder im Client-Setup-Assistenten gesteuert.

- **Application Policy Management-Optionen**: Sie zeigen dieses Dialogfeld an, indem Sie zuerst auf die Option **APM-Client in festgelegten Zeitabständen starten** und anschließend auf die Schaltfläche **Konfigurieren** klicken.
- **Local Scheduler-Zeitfilteroptionen**: Sie zeigen dieses Dialogfeld an, indem Sie im Dialogfeld "Application Policy Management-Optionen" auf die Schaltfläche **Zeitfilter** klicken.

Das Dialogfeld "Application Policy Management-Optionen" enthält die Option **APM-Client periodisch ausführen**. Mit dieser Option wird der Local Scheduler-Agent angewiesen, den Task in den von Ihnen angegebenen Zeitabständen auszuführen. Falls Sie diese Option nicht auswählen, wird Application Policy Management nur zur einmaligen Ausführung eingeplant.

Wenn Sie die Option **APM-Client periodisch ausführen** auswählen, müssen Sie ein **Ausführungsintervall** für die tägliche, wöchentliche oder monatliche Ausführung der Task angeben. Dieses Intervall beginnt zu dem Zeitpunkt, an dem der Local Scheduler-Agent den Task zum ersten Mal ausführt. Wenn Sie beispielsweise "Wöchentlich" auswählen, führt der Local Scheduler den Task aus, sobald sich die erste Gelegenheit dazu bietet. Wenn der Scheduler den Task zum ersten Mal an einem Dienstag ausführt, wird er sie im Allgemeinen jeden Dienstag ausführen.

Zur genaueren Bestimmung des Ausführungszeitpunkts der Task verwenden Sie das Dialogfeld "Zeitfilteroptionen". Sie können maximal drei Filter festlegen, um zu definieren, wann der Task ausgeführt wird.

- Tageszeitfilter
- Wochentagfilter
- Monatsdatumfilter

Diese Filter definieren das von Ihnen angegebene Ausführungsintervall (täglich, wöchentlich, monatlich) genauer. Wenn Sie beispielsweise das Ausführungsintervall "Monatlich" einstellen und als Monatsdatumfilter den Zeitraum vom 21. bis zum 22. festlegen, führt der Local Scheduler den Task einmal monatlich irgendwann zwischen dem 21. und 22. des Monats aus.

Sie können einen oder mehrere Filter für das Ausführungsintervall definieren, müssen jedoch sicherstellen, dass die Filter für das gewählte Intervall sinnvoll sind. Wenn Sie z. B. das Ausführungsintervall "Täglich" wählen und dann einen Tageszeitfilter für den Zeitraum zwischen 20:00 und 23:00 Uhr sowie einen Wochentagfilter für "Montag" hinzufügen, wird der Task keineswegs täglich ausgeführt, sondern lediglich jeden Montag zwischen 20:00 und 23:00 Uhr.

Wenn Sie im Dialogfeld "Clientsetup: Application Policy Management-Optionen" einen Bandbreitenfilter verwenden, bestimmt auch dieser, wann der Local Scheduler den Task ausführt. Die Kriterien für Zeit- und Bandbreitenfilter müssen erfüllt sein, damit der Local Scheduler den Task ausführt. Angenommen, Sie haben festgelegt, dass der Task einmal pro Woche am Mittwoch ausgeführt werden soll, und zudem als Bandbreitenfilter eine Hochgeschwindigkeitsverbindung angegeben. Wenn der Client am Mittwoch eine Wählverbindung herstellt, wird der Task nicht ausgeführt, obwohl das Zeitfilterkriterium erfüllt ist.

Verteilen der Bandbreitenerkennung

Die Bandbreitenerkennung ermöglicht die Bandbreitenerkennung zwischen Clients und Core Server. Sie können Management Suite-Aktionen, wie z. B. Software Distribution, von der verfügbaren Bandbreite abhängig machen. Verwenden Sie diese Option, wenn Fernclients oder Clients vorhanden sind, die über eine langsame Verbindung eine Netzwerkverbindung herstellen.

Verteilen benutzerdefinierter Datenformulare

Sie können benutzerdefinierte Datenformulare erstellen und verteilen, um Clientdaten zu erfassen, die die in der Core-Datenbank verfügbaren Standardinformationen ergänzen. Die Formulare, die Sie mit dem Form Designer anlegen, können mit einem Clientverteilungsdienst oder mit dem Client-Setup-Assistenten verteilt werden.

Benutzerdefinierte Formulare erfordern die Komponente "Bestandsaufnahme".

Passen Sie die Formulare, die Sie an Clients in Ihrer Verwaltungsdomäne verteilen, mit dem Form Designer an. Weitere Informationen finden Sie unter "Verwenden von benutzerdefinierten Datenformularen" in Kapitel 4.

Informationen zum Client-Setup-Assistenten: Seite "Benutzerdefinierte Datenformulare"

Clientsetup: Der Bereich "Benutzerdefinierte Datenformulare" besteht aus zwei Seiten und wird nur angezeigt, wenn Sie auf der Seite "Komponenten installieren" "Benutzerdefinierte Datenformulare" aktiviert haben.

Die erste Seite enthält die folgenden Funktionen:

- **Manuelle Aktualisierung:** Ausgewählte Formulare werden an alle Clients versendet. Wenn sich die Formulare ändern, oder neue Formulare hinzugefügt werden, müssen Sie diese manuell an die Fernclients senden.
- **Automatische Aktualisierung:** Die Fernclients suchen jedes Mal, wenn der Inventarscan ausgeführt wird, z. B. beim Start, auf dem Core Server nach aktualisierten Formularen. Auf jedem Client muss ein Laufwerk dem Verzeichnis LDLOGON auf dem Core Server zugewiesen sein, damit der Client auf die aktualisierten Formulare zugreifen kann.
- **Formulare anzeigen:** Wählen Sie aus, wie Fernclients auf benutzerdefinierte Formulare zugreifen:
  - **Beim Start:** Die ausgewählten Formulare werden automatisch beim Start auf allen Clients ausgeführt.
  - **Während der Inventarscanner ausgeführt wird:** Die ausgewählten Formulare werden nur ausgeführt, wenn der Inventarscanner auf den Clients ausgeführt wird. Der Inventarscanner wird automatisch beim Start ausgeführt und kann jederzeit manuell von den Clients ausgeführt werden.
  - **Nur im LANDesk-Programmordner:** Die ausgewählten Formulare werden als Elemente im LANDesk Management-Ordner des Client angezeigt. Sie werden nicht automatisch ausgeführt.

Die zweite Seite enthält alle festgelegten benutzerdefinierten Datenformulare. Markieren Sie die Formulare, die Clients zur Verfügung stehen sollen, die die entsprechende Konfigurations-Task erhalten.

Informationen zum Client-Setup-Assistenten: Seite "Verfügbare Formulare"

Clientsetup: Der Bereich "Benutzerdefinierte Datenformulare" besteht aus zwei Seiten und wird nur angezeigt, wenn Sie auf der Seite "Komponenten installieren" "Benutzerdefinierte Datenformulare" aktiviert haben.

Wählen Sie auf der zweiten Seite die Formulare aus, die Sie verteilen möchten. Sie müssen zuerst Formulare erstellen (unter **Extras | Benutzerdefinierte Datenformulare**), bevor sie in der Liste angezeigt werden.

Aktivieren von Migrationstasks

Mit der Client Setup-Option "Migrationstasks" werden die Komponenten ausgewählt, die für die Betriebssystem-Verteilung und Profilmigration notwendig sind. Die Option "Migrationstasks" stellt lediglich eine Möglichkeit dar, die Komponenten Bandbreitenerkennung, Common Base Agent und Enhanced Software Distribution schnell auszuwählen. Falls Sie diese Komponenten bereits ausgewählt haben, bewirkt die Auswahl der Option "Migrationstasks" nichts.

Verteilen von Enhanced Software Distribution

Enhanced Software Distribution automatisiert die Installation von Softwareanwendungen und die Verteilung von Dateien an Clients. Verwenden Sie diesen Agenten, um Anwendungen gleichzeitig auf mehreren Clients zu installieren oder um Dateien oder Treiber auf mehreren Clients zu aktualisieren.

Enhanced Software Distribution benutzt einen Web- oder Dateiserver zum Speichern der Pakete. Die Clients greifen beim Herunterladen eines Pakets auf diesen Paketserver zu. Sie müssen, wie in Kapitel "Enhanced Software Distribution" des *Benutzerhandbuchs* beschrieben, einen Paketserver konfigurieren. Sie können den Enhanced Software Distribution-Agenten an Clients verteilen, bevor Sie einen Paketserver einrichten.

Konfigurieren von Clients für Enhanced Software Distribution

Der Client-Setup-Assistent enthält keine speziellen Seiten für Enhanced Software Distribution.

Enhanced Software Distribution erfordert die Komponenten Bandbreitenerkennung und Common Base Agent.

Verteilen von Local Scheduler

Der Local Scheduler-Agent ermöglicht es der Management Suite, Client-Tasks abhängig von der Tageszeit oder der verfügbaren Bandbreite zu starten. Der Local Scheduler-Agent ist besonders für mobile Computer nützlich, die nicht ständig mit dem Netzwerk verbunden sind oder die Netzwerkverbindung über eine Wählverbindung herstellen. Sie können beispielsweise Local Scheduler verwenden, um eine Paketverteilung an mobile Computer nur dann zuzulassen, wenn diese Clients mit dem WAN verbunden sind.

Beim Planen der Verteilung von Enhanced Software Distribution-Paketen und bei der Definition von Anwendungsrichtlinien können Sie angeben, welche Bandbreite für die Verteilung der Pakete bzw. die Anwendung der Richtlinien erforderlich ist.

Der Local Scheduler wird unter Windows NT/2000/XP als Dienst und unter Windows 95/98 als Pseudodienst ausgeführt.

Local Scheduler erfordert die Komponente Bandbreitenerkennung.

Informationen zum Client-Setup-Assistenten: Seite "Local Scheduler"

Client-Setup: Die Seite "Local Scheduler" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" den "Local Scheduler" ausgewählt haben. Die Seite enthält die folgenden Funktionen:

- **Zeitabstand in Sekunden, in dem der Local Scheduler-Client ein Polling nach ausführbereiten Tasks durchführt:** Gibt an, wie oft der Local Scheduler nach Tasks sucht. Der Standardwert ist 30 Sekunden. Das von Ihnen ausgewählte Polling-Intervall wird auf dem lokalen Computer gespeichert.
- **Zeitabstand für Bandbreitenerkennung, in Sekunden:** Gibt an, wie oft der Local Scheduler die Bandbreite überprüfen soll. Der Standardwert ist 120 Sekunden. Bandbreitenüberprüfungen finden nur statt, wenn eine geplante Task ansteht.

Verteilen der Softwarelizenzüberwachung

Der Softwarelizenzüberwachungsagent ermöglicht es Ihnen, die Einhaltung von Lizenzbestimmungen, die Verwendung von Produkten und Ablehnungstendenzen bei Clients in Ihrem Netzwerk zu überwachen. Der Agent zeichnet Daten über alle auf einem Client installierten Anwendungen auf und speichert diese Daten in der Systemregistrierung des Clients. Im Fenster "Softwarelizenzüberwachung" können Sie festlegen, dass die wichtigsten dieser installierten Anwendungen überwacht werden. Daten zur Verwendung von nicht überwachten Anwendungen werden ignoriert und in der Systemregistrierung des Clients schließlich durch neuere Daten überschrieben.

Nachdem Sie die zu überwachenden Anwendungen und Lizenzen angegeben haben, geschieht Folgendes:

- Management Suite sucht nach Clients, auf denen die zu überwachenden Anwendungen ausgeführt werden, und importiert diese Liste in das Fenster "Softwarelizenzüberwachung". Diese Clientliste bleibt unverändert, bis der nächste Softwarescan durchgeführt wird.
- Während der nächsten Überprüfung liest der Scanner die vom Softwarelizenzüberwachungsagenten erfassten Clientdaten und sendet diese an den Core Server. Management Suite aktualisiert dann das Fenster "Softwarelizenzüberwachung" mit den Daten zu den überwachten Lizenzen und Produkten.

Bei mobilen Clients, die vom Netzwerk getrennt sind, erfasst der Softwarelizenzüberwachungsagent weiterhin Daten und speichert diese in der Systemregistrierung des Clients. Sobald der Client wieder eine Netzwerkverbindung hergestellt hat, wird bei der nächsten Überprüfung erkannt, welche der zwischengespeicherten Daten überwacht werden, und diese Daten werden an den Core Server gesendet. Das Fenster "Softwarelizenzüberwachung" wird daraufhin mit den neuesten Daten zur Einhaltung von Lizenzbestimmungen sowie zur Verwendung und zur Verweigerung für diese mobilen Clients aktualisiert. Die Softwarelizenzüberwachung erfordert die Komponente Bestandsaufnahme.

Verteilen von Targeted Multicast

Mit Targeted Multicast können Sie Softwarepakete an mehrere Clients übertragen, ohne die Routerkonfiguration ändern zu müssen. Diese Methode funktioniert mit den vorhandenen Softwareverteilungspaketen. Wenn Sie Targeted Multicast verwenden, ist das Verteilen der Software ganz einfach, selbst in WAN-Umgebungen mit mehreren Hops und niedrigen Verbindungsgeschwindigkeiten (56 KBit/s). Targeted Multicast verwendet HTTP für die Übermittlung von einer Website an einen Subnetzrepräsentanten. Der Management Suite-Inventardienst stellt dem Targeted Multicast-Dienst alle Subnetzinformationen zur Verfügung.

Targeted Multicast bietet zahlreiche Vorteile, die Standard-Multicast-Methoden nicht aufweisen. Mithilfe der inventarbasierten Angabe von Clients können Sie ein Paket über ein Broadcast an eine ausgewählte Gruppe von Computern, die bestimmte Kriterien erfüllen, senden. Mit Targeted Multicast wird das Verfahren auch deshalb vereinfacht, weil Router nicht extra für die Verarbeitung von übermittelten Paketen konfiguriert werden müssen.

Target Multicasting stellt in der Management Suite die Standardmethode für die Softwaredistribution dar. Das sollten Sie auch nicht ändern. Falls Sie diese Methode dennoch ausschalten möchten, deaktivieren Sie die Option **Dieses Paket mit Multicast verteilen** im Dialogfeld "Skript erstellen", das beim Erstellen eines Verteilungspaket-Skripts angezeigt wird.

Verteilen des Agenten "Taskfertigstellen"

Der Agent "Taskfertigstellen" überprüft den Core Server darauf hin, ob geplante Aufträge vorliegen, die vom Client auszuführen sind. "Taskfertigstellen" ist besonders für mobile Benutzer hilfreich, die nicht ständig mit dem Netzwerk verbunden sind und die Ausführung geplanter Aufträge übersehen können.

Während seiner Ausführung öffnet der Agent "Taskfertigstellen" auf den Clients ein Statusfenster, solange er den Core Server überprüft. Dieses Fenster wird per Voreinstellung nach 15 Sekunden wieder geschlossen. Sie können angeben, dass der Agent "Taskfertigstellen" periodisch oder nur in bestimmten Zeiträumen/Tagen/Wochen/Monaten ausgeführt werden soll. Wenn der Computer während der Ausführung des Agenten "Taskfertigstellen" nicht mit dem Netzwerk verbunden ist oder nicht mit dem Core Server kommunizieren kann, dann wird die Ausführung des Task Completion-Agenten beendet.

"Taskfertigstellen" erfordert die Komponenten Bandbreitenerkennung, Common Base Agent und Enhanced Software Distribution.

Weitere Informationen zum Planen der Ausführung des Agenten "Taskfertigstellen" finden Sie weiter oben in diesem Kapitel unter "Starten des APM-Clients in festgelegten Zeitabständen". Die in diesem Abschnitt gegebenen Informationen gelten auch für den Agenten "Taskfertigstellen".

Informationen zum Client-Setup-Assistenten: Seite "Taskfertigstellen"

Clientsetup: Die Seite "Taskfertigstellen" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" die Option "Taskfertigstellen" ausgewählt haben. Der Agent "Taskfertigstellen" überprüft den Core Server darauf hin, ob geplante Aufträge vorliegen, die vom Client auszuführen sind. "Taskfertigstellen" ist besonders für mobile Benutzer hilfreich, die nicht ständig mit dem Netzwerk verbunden sind und die Ausführung geplanter Aufträge übersehen können.

Während seiner Ausführung öffnet der Agent "Taskfertigstellen" auf den Clients ein Statusfenster, solange er den Core Server überprüft. Dieses Fenster wird per Voreinstellung nach 15 Sekunden wieder geschlossen.

Sie können außerdem angeben, dass der Agent "Taskfertigstellen" periodisch oder nur in bestimmten Zeiträumen/Tagen/Wochen/Monaten ausgeführt werden soll.

Wenn der Computer während der Ausführung des Agenten "Taskfertigstellen" nicht mit dem Netzwerk verbunden ist oder nicht mit dem Core Server kommunizieren kann, wird die Ausführung des Agenten "Taskfertigstellen" beendet.

Die Seite enthält die folgenden Funktionen:

- **Den Client "Taskfertigstellen" bei jeder Benutzeranmeldung starten:** Der Client "Taskfertigstellen" wird zur Startgruppe hinzugefügt.
- **Den Client "Taskfertigstellen" in festgelegten Zeitabständen starten (Local Scheduler für Clients erforderlich):** Hier können Sie angeben, wann der Client "Taskfertigstellen" ausgeführt werden soll.
- **Vollständige Benutzeroberfläche:** Das Fenster "Taskfertigstellen" wird auf den Clients immer angezeigt, wenn "Taskfertigstellen" ausgeführt wird.
- **Benutzeroberfläche nur bei ausstehenden Tasks anzeigen:** Das Fenster "Taskfertigstellen" wird nur angezeigt, wenn noch Tasks ausgeführt werden müssen.
- **Ausführung im Hintergrund:** Das Fenster "Taskfertigstellen" wird auf den Clients nie angezeigt.

Informationen zum Client-Setup-Assistenten: Seite "Taskfertigstellungsoptionen"

Clientsetup: Die Seite "Taskfertigstellen" wird angezeigt, wenn Sie auf der Seite "Komponenten installieren" die Option "Taskfertigstellen" ausgewählt haben. Klicken Sie auf die Schaltfläche **Konfigurieren**, um das Dialogfeld "Taskfertigstellungsoptionen" zu öffnen.

Wenn der Agent "Taskfertigstellen" regelmäßig ausgeführt werden soll, klicken Sie in diesem Dialogfeld auf die Schaltfläche **Zeitfilter**.

Die Seite enthält die folgenden Funktionen:

- **Den Client "Taskfertigstellen" periodisch starten:** Sie können festlegen, wie häufig "Taskfertigstellen" auf dem Core Server nach Tasks sucht. Aktivieren Sie diese Option und wählen Sie ein **Ausführungsintervall** aus dem Listenfeld. Der Agent wird einmal in dem von Ihnen angegebenen Intervall ausgeführt. Wenn Sie diese Option wählen, klicken Sie auf die Schaltfläche **Zeitfilter** und richten Sie die Intervalldetails ein. Der Benutzer muss sich anmelden, damit der Agent ausgeführt wird.
- **Alle Netzwerkverbindungen zulassen:** "Taskfertigstellen" wird unabhängig von der Verbindungsart der Clients ausgeführt. Wenn alle Ihre Clients über einen Hochgeschwindigkeits-Netzwerkzugriff auf den Paketserver verfügen, ist diese Option empfehlenswert.
- **Alle Nicht-RAS-Netzwerkverbindungen zulassen:** "Taskfertigstellen" wird ausgeführt, wenn die Clientverbindung mit dem Paketserver mindestens WAN-Geschwindigkeit, aber nicht LAN-Geschwindigkeit erreicht. Die LAN-Geschwindigkeit ist standardmäßig als 262.144 Bit/s definiert.
- **Nur Hochgeschwindigkeitsverbindung zulassen:** "Taskfertigstellen" wird ausgeführt, wenn die Clientverbindung mit dem Paketserver die LAN-Geschwindigkeitseinstellung (standardmäßig 262.144 Bit/s) übertrifft.

Informationen zum Client-Setup-Assistenten: Seite "Neustartoptionen"

Clientsetup: Die Seite "Neustartoptionen" wird immer angezeigt. Die Seite enthält die folgenden Funktionen:

- **Clients nach Konfiguration nicht neu starten:** Die Clients werden nicht neu gestartet, auch wenn die ausgewählten Komponenten einen Neustart erfordern. Wenn ein Neustart erforderlich ist, funktionieren die Komponenten erst richtig, wenn der Client neu gestartet wurde.
- **Clients bei Bedarf neu starten:** Die Clients werden nur neu gestartet, wenn eine ausgewählte Komponente einen Neustart erfordert.
- **Neustart mit Option zum Abbruch:** Falls eine ausgewählte Komponente einen Neustart erfordert, können die Clients diesen abbrechen. Wenn ein Neustart erforderlich ist, funktionieren die Komponenten erst richtig, wenn der Client neu gestartet wurde. Sie können festlegen, wie lange die Aufforderung zum Neustart auf dem Bildschirm des Client angezeigt wird, ehe der Computer neu gestartet wird. Dieses Timeout ist für Benutzer sinnvoll, die während der Clientverteilung nicht an ihrem Computer sitzen.

Informationen zum Client-Setup-Assistenten: Informationsseite "Neustart"

Clientsetup: Die Seite "Neustartoptionen" wird immer angezeigt. Sie soll Sie daran erinnern, dass die Neustartoptionen nur für Client Setup-Verteilungen gelten, die als geplante Tasks ausgeführt werden.

Informationen zum Client-Setup-Assistenten: Seite "Fertig"

Die Seite "Fertig" wird angezeigt, sobald Sie alle Seiten des Assistenten abgeschlossen haben. Auf dieser Seite können Sie die erstellte Konfiguration als Standardkonfiguration festlegen. Damit ist sie die Standardkonfiguration für die Erstellung einer neuen Konfiguration. Außerdem wird sie für die Neukonfiguration vorhandener Clients verwendet, die Anmeldeskripts auf dem Core Server verwenden.

Im Client-Setup-Assistenten können Sie auch ein selbstextrahierendes Enhanced Software Distribution-(ESWD)-Paket erstellen, das Sie an die Clients verteilen. Auf den Clients muss der Enhanced Software Distribution-Agent installiert sein, damit diese Funktion verwendet werden kann.

Sie können auch über Targeted Multicast aktualisierte Client-Konfigurationspakete an mehrere Computer gleichzeitig senden; gleichzeitig wird der Bedarf an Netzwerkbandbreite gesenkt. Weitere Informationen finden Sie unter "Verwenden von Targeted Multicasting mit Enhanced Software Distribution" in Kapitel 6.

So erstellen Sie ein Softwareverteilungspaket

1. Erstellen Sie eine Clientkonfiguration
2. Wählen Sie auf der Seite **Fertig** im Client-Setup-Assistenten **ESWD-Paket erstellen** aus.
3. Klicken Sie auf **Fertigstellen**.
4. Wählen Sie im Browser **Enhanced Software Distribution-Paket speichern unter** und wählen Sie anschließend einen Dateinamen und einen Speicherort für das Paket aus. Beachten Sie, dass das Standardverzeichnis LDMAIN ist. Clients haben keinen Zugriff auf dieses Verzeichnis. Wählen Sie ein Verzeichnis, in dem Sie Pakete speichern, und auf das die Clients zugreifen können.
5. Klicken Sie auf **Speichern**. Der Assistent erstellt das selbstextrahierende .EXE-Paket.

Informationen zum Dialogfeld "Client Setup-Dienstprogramm"

Das Dialogfeld "Client Setup-Dienstprogramm" zeigt den Status eines geplanten Clientkonfigurations-Task während der Verarbeitung an. Es dient nur Ihrer Information. Die zu konfigurierenden Clients wurden bereits bei der Planung des Task ausgewählt.

Das Dialogfeld "Client Setup-Dienstprogramm" enthält die folgenden Funktionen:

- **Zu konfigurierende Clients:** Führt die Clients auf, die die Konfigurationseinstellungen erhalten sollen.
- **Clients, die konfiguriert werden:** Führt die Clients auf, die von der Konsole kontaktiert wurden und die gerade mit dieser Einstellungsdatei konfiguriert werden.

- **Konfigurierte Clients:** Führt die Clients auf, die die Konsole während dieser geplanten Sitzung konfiguriert hat. Wenn der Konfigurationsversuch erfolgreich war, ist der Status "Abgeschlossen". Falls der Konfigurationsversuch aus irgendeinem Grund fehlgeschlagen ist, lautet der Status "Fehlgeschlagen". Diese Stati sind auch im Fenster "Geplante Tasks" enthalten, wenn die entsprechende Task ausgewählt ist.
- **Konfigurationsdateien werden erstellt:** Zeigt eine Statusleiste mit dem Abschlussstatus der kompletten Konfigurations-Task an.

Einrichten eines Clientverteilung-Service Centers

Das Clientverteilung-Service Center bietet eine einfache Methode für das Verteilen von LANDesk-Agenten auf Windows-Clients. Wenn Sie einen Clientverteilungs-Dienst einrichten, werden automatisch Anmeldeskripts erstellt. Sie müssen dann den Clients das entsprechende Skript zuweisen, damit sie konfiguriert werden können.

Im Einklang mit der stufenweisen Verteilungsstrategie sollten Sie zunächst die Dienste begrenzen, die auf die Clients verteilt werden. Für den anfänglichen Rollout empfehlen wir, dass Sie eine Clientkonfiguration erstellen, die den CBA umfasst (den Agenten, der die Kommunikation mit dem Core Server ermöglicht), den Fernsteuerungsagenten und den Inventaragenten.

Der Service Center-Assistent verwendet die Einstellung für jede Komponente, die Sie im Client-Setup-Assistenten einrichten. Im Client-Setup-Assistenten können Sie die Einstellungen für jede Komponente festlegen, die Sie verteilen. Wenn Sie diese Einstellungen nicht im Client-Setup-Assistenten einrichten, bevor Sie den Service Center-Assistenten ausführen, werden die Standardeinstellungen verwendet.

Wenn auf dem Client Windows NT/2000/2003/XP ausgeführt wird
Benutzer müssen über Administratorrechte auf ihren Arbeitsplatzrechnern verfügen, um Agenten mit einem Anmeldeskript zu installieren. Wenn Benutzer über keine Administratorrechte verfügen, können Sie die Push-Konfigurationsmethode verwenden.

So erstellen Sie eine Clientkonfiguration

1. Klicken Sie in der Konsole auf **Extras | Clientsetup**.
2. Doppelklicken Sie auf das Symbol **Clientkonfiguration hinzufügen**.
3. Wählen Sie auf der Seite des Client-Setup-Assistenten "Komponenten installieren" den **Common Base Agent**, den **Inventarscanner** und die **Fernsteuerungskomponenten**.
4. Gehen Sie die verschiedenen Seiten durch, indem Sie auf **Weiter** klicken, und nehmen Sie die notwendigen Änderungen darin vor. Klicken Sie auf **Hilfe**, um Informationen über jede Seite anzuzeigen.
5. Klicken Sie am Ende des Assistenten auf **Als Standardkonfiguration festlegen**.
6. Klicken Sie auf **Fertigstellen**, um den Assistenten zu beenden.

Weitere Informationen über das Einrichten von Clientverteilung-Service Center finden Sie in Stufe 4 im *Verteilungshandbuch*.

Kapitel 3: Verwenden von Abfragen

Abfragen sind benutzerdefinierte Suchen in Ihren Core-Datenbanken. LANDesk Management Suite enthält Tools, mit denen Sie mithilfe von Datenbankabfragen Client-Abfragen in der Core-Datenbank und mithilfe von LDAP-Abfragen Client-Abfragen in anderen Verzeichnissen durchführen können. Core-Datenbanken erstellen Sie in der Netzwerkansicht der Konsole. LDAP-Abfragen erstellen Sie mit dem Tool Directory Manager.

In diesem Kapitel erfahren Sie mehr über:

Management Suite-Abfragen

- Abfragenübersicht
- Abfragegruppen
- Erstellen von Datenbankabfragen
- Ausführen von Abfragen
- Importieren und Exportieren von Abfragen

LDAP-Abfragen mit Directory Manager

- Verwenden von Directory Manager für die Abfrage von Verzeichnissen über LDAP
- Informationen zum Directory Manager-Fenster
- Erstellen von LDAP-Verzeichnisabfragen
- Informationen über LDAP

Abfragenübersicht

Abfragen helfen Ihnen bei der Netzwerkverwaltung, indem Sie mithilfe von System- oder Benutzerkriterien nach Netzwerkgeräten in der Core-Datenbank suchen und diese organisieren können.

So können Sie beispielsweise eine Abfrage erstellen und ausführen, die nur Clients mit einer Taktgeschwindigkeit von weniger als 166 MHz, weniger als 64 MB Arbeitsspeicher oder einer Festplatte mit weniger als 2 GB Speicherkapazität erfasst. Erstellen Sie eine oder mehrere Abfrageanweisungen für diese Bedingungen und verknüpfen Sie diese Anweisungen mithilfe von logischen Operatoren. Wenn die Abfragen ausgeführt wurden, können Sie die Ergebnisse drucken, auf die entsprechenden Clients zugreifen und sie verwalten.

Abfragegruppen

Abfragen können in der Netzwerkansicht in Gruppen organisiert werden. Erstellen Sie neue Abfragen (und neue Abfragegruppen), indem Sie mit der rechten Maustaste entweder auf die Gruppe "Eigene Abfragen" klicken und **Neue Abfrage** oder **Neue Gruppe** auswählen.

Ein Management Suite-Administrator (Benutzer mit LANDesk-Administratorrechten) kann den Inhalt aller Abfragegruppen anzeigen. Dazu gehören: "Eigene Abfragen", "Öffentliche Abfragen", "Alle Abfragen" und "Benutzerabfragen".

Wenn sich andere Management Suite-Benutzer bei der Konsole anmelden, können sie basierend auf ihrem Gerätebereich Abfragen in den Gruppen "Eigene Abfragen", "Öffentliche Abfragen" und "Alle Abfragen" anzeigen. Ein normaler Benutzer kann die Gruppe "Benutzerabfragen" nicht anzeigen.

Wenn Sie eine Abfrage in eine Gruppe verschieben (durch Klicken mit der rechten Maustaste und Auswählen von **Zu neuer Gruppe hinzufügen** oder **Zur vorhandenen Gruppe hinzufügen** bzw. durch Ziehen und Ablegen der Abfrage), erstellen Sie eine Kopie der Abfrage. Sie können die Kopie in jeder Abfragegruppe ändern oder löschen, die Masterkopie der Abfrage (in der Gruppe "Alle Abfragen") bleibt davon unberührt.

Ein Administrator muss auf die Gruppe "Benutzerabfragen" in der Konsole doppelklicken, damit die Abfragen zur Gruppe hinzugefügt werden
Nach dem Erstellen von Benutzern und dem Zuweisen von Rechten und Bereichen muss der Core-Administrator auf die Gruppe "Benutzerabfragen" doppelklicken, um sicherzustellen, dass alle privaten gespeicherten Abfragen unter der Gruppe "Benutzerabfragen" gespeichert werden. Dies muss nur einmal getan werden. Alle privaten Abfragen, die vor der Durchführung des obigen Schritts erstellt werden, gelangen in die Gruppe "Alle Abfragen".

Weitere Informationen zur Anzeige von Abfragegruppen und Abfragen in der Netzwerkansicht und zu ihrer Verwendung finden Sie unter "Erläuterungen zur Netzwerkansicht" in Kapitel 1.

Erstellen von Datenbankabfragen

Verwenden Sie das Dialogfeld "Neue Abfrage", um eine Query durch Auswählen von Attributen, relationalen Operatoren und Attributwerten zu erstellen. Erstellen Sie eine Abfrageanweisung, indem Sie ein Inventarattribut auswählen und es mit einem akzeptablen Wert verknüpfen. Verknüpfen Sie die Abfrageanweisungen logisch miteinander, um sicherzustellen, dass Sie als Gruppe ausgewertet werden, bevor Sie sie mit anderen Anweisungen oder Gruppen verknüpfen.

So erstellen Sie eine Datenbankabfrage

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf die Gruppe **Eigene Abfragen** (oder auf **Öffentliche Abfragen**, wenn Sie über die Public Query Management-Berechtigung verfügen) und anschließend auf **Neue Abfrage**.
2. Geben Sie einen eindeutigen Namen für die Abfrage ein.
3. Wählen Sie eine Komponente aus der Inventarattributliste.
4. Wählen Sie einen relationalen Operatoren.
5. Wählen Sie einen Wert aus der Werteliste. Sie können den Wert bearbeiten.
6. Klicken Sie auf **Einfügen**, um die Anweisung in die Abfrageliste aufzunehmen.
7. Wenn Sie eine Abfrage für mehrere Komponenten ausführen möchten, klicken Sie auf einen logischen Operatoren (AND, OR) und wiederholen Schritte 2 bis 5.
8. (Optional) Um Abfrageanweisungen so zu gruppieren, dass sie als Gruppe ausgewertet werden, wählen Sie zwei oder mehrere Abfrageanweisungen und klicken auf **Gruppe( )**.
9. Wenn Sie alle Anweisungen hinzugefügt haben, klicken Sie auf **Speichern**.

Informationen zum Dialogfeld "Neue Abfrage"

Mithilfe dieses Dialogfeldes erstellen Sie eine neue Abfrage mit den folgenden Funktionen:

- **Name:** Identifiziert die Abfrage in Abfragegruppen.
- **Rechnerkomponenten:** Führt die Inventarkomponenten und Attribute auf, nach denen die Abfrage scannt.
- **Relationale Operatoren:** Listet relationale Operatoren auf. Diese Operatoren bestimmen, welche Beschreibungswerte für eine bestimmte Komponente die Abfrage erfüllen.

  Der Operator Gleich ist ein neuer relationaler Operator. Wenn Sie in ihrer Abfrage keine Platzhalter (*) angeben, fügt der Operator Gleich an beiden Enden der Zeichenfolge Platzhalter hinzu. Hier drei Beispiele für die Verwendung des Operators Gleich:
  Abfrage Computer.Anzeigename GLEICH "Eigener Rechner": Abfrage Computer.Anzeigename GLEICH "%Al's Rechner%"
  Computer.Anzeigename GLEICH "Al's Rechner*": Abfrage Computer.Anzeigename GLEICH "Al's Rechner%"
  Computer.Anzeigename GLEICH "*Al's Rechner": Computer.Anzeigename GLEICH "%Al's Rechner"

- **Geprüfte Werte anzeigen:** Führt akzeptable Werte für das ausgewählte Inventarattribut auf. Sie können den entsprechenden Wert auch manuell eingeben oder einen ausgewählten Wert mit dem Wertefeld "Bearbeiten" modifizieren. Wenn der ausgewählte relationale Operator "Besteht" oder "Ist nicht vorhanden" lautet, sind keine Beschreibungswerte möglich.
- **Logischer Operator:** Legt fest, wie Abfrageanweisungen logisch miteinander in Beziehung stehen:
    - **AND:** Sowohl die vorherige Abfrageanweisung als auch die einzufügende Anweisung müssen wahr sein, um die Abfrage zu erfüllen.
    - **OR:** Entweder die vorherige Abfrageanweisung oder die einzufügende Anweisung müssen wahr sein, um die Abfrage zu erfüllen.
- **Einfügen:** Fügt die neue Anweisung in die Abfrageliste ein und setzt sie entsprechend des aufgeführten logischen Operators in eine logische Beziehung zu den anderen Anweisungen. Sie können diese Schaltfläche erst betätigen, wenn Sie eine akzeptable Abfrageanweisung erstellt haben.
- **Bearbeiten:** Lässt Sie die Abfrageanweisung bearbeiten. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche **Aktualisierung**.
- **Löschen:** Löscht die ausgewählte Anweisung aus der Abfrageliste.
- **Alle löschen:** Löscht alle Anweisungen aus der Abfrageliste.
- **Abfrageliste:** Führt jede in die Abfrage eingefügte Anweisung und die logische Beziehung zu anderen aufgeführten Anweisungen auf. Gruppierte Anweisungen sind von Klammern umgeben.
- **Gruppe ():** Fasst die ausgewählten Anweisungen in einer Gruppe zusammen, sodass sie als Gruppe ausgewertet werden, bevor Sie auf andere Anweisungen angewendet werden.
- **Gruppierung aufheben:** Hebt die Gruppierung der ausgewählten gruppierten Anweisungen auf.
- **Filter:** Öffnet das Dialogfeld "Abfragefilter", das Gerätegruppen anzeigt. Wenn Sie Gerätegruppen auswählen, beschränken Sie die Abfrage nur auf die Clients, die in den ausgewählten Gruppen enthalten sind. Wenn Sie keine Gruppen auswählen, ignoriert die Abfrage die Gruppenmitgliedschaft.
- **Spalten auswählen:** Lässt Sie Spalten hinzufügen und entfernen, die in der Abfrageergebnisliste dieser Abfrage angezeigt werden. Wählen Sie eine Komponente und klicken Sie auf die Schaltfläche mit dem Pfeil nach rechts, um sie zur Spaltenliste hinzuzufügen. Sie können den Text für Alias und Sortierreihenfolge manuell bearbeiten. Ihre Änderungen werden in der Abfrageergebnisliste angezeigt.
- **Speichern:** Speichert die aktuelle Abfrage. Wenn Sie eine Abfrage speichern, bevor Sie sie ausführen, wird sie in der Core-Datenbank gespeichert und ist dort vorhanden, bis Sie sie löschen.

Abfrageanweisungen werden in der gezeigten Reihenfolge ausgeführt. Wenn keine Gruppierungen vorgenommen werden, werden die in diesem Dialogfeld aufgeführten Abfrageanweisungen von unten nach oben ausgeführt. Fassen Sie miteinander in Bezug stehende Elemente in Gruppen zusammen, sodass sie als Gruppe ausgewertet werden; andernfalls fallen die Ergebnisse Ihrer Abfrage eventuell anders als erwartet aus.

Ausführen von Datenbankabfragen

So führen Sie eine Abfrage aus

1. Erweitern Sie in der Netzwerkansicht die Abfragegruppen, so dass Sie die auszuführende Abfrage suchen können.
2. Klicken Sie doppelt auf die Abfrage. Alternativ dazu können Sie auch mit der rechten Maustaste klicken und **Ausführen** wählen.
3. Die Ergebnisse (passenden Geräte) werden im rechten Fensterbereich der Netzwerkansicht angezeigt.

Importieren und Exportieren von Abfragen

Sie können über die Import- und Exportfunktionen Abfragen aus einer Core-Datenbank in eine andere übertragen. Sie können exportierte Abfragen aus Management Suite 8 und der Webkonsole als .XML-Dateien importieren. Exportierte Abfragen aus Management Suite 6.52, 6.62 und 7.0 können Sie als .QRY-Dateien importieren.

So importieren Sie eine Abfrage

1. Klicken Sie mit der rechten Maustaste auf die Abfragegruppe, in welche die Abfrage importiert werden soll.
2. Wählen Sie **Importieren** aus dem Kontextmenü.
3. Navigieren Sie zur Abfrage, die Sie importieren möchten, und wählen Sie sie aus.
4. Klicken Sie auf **Öffnen**, um die Abfrage zur ausgewählten Abfragegruppe in der Netzwerkansicht hinzuzufügen.

So exportieren Sie eine Abfrage

1. Klicken Sie mit der rechten Maustaste auf die zu exportierende Abfrage.
2. Wählen Sie **Exportieren** aus dem Kontextmenü.
3. Navigieren Sie zu dem Ort, an dem Sie die Abfrage (als .XML-Datei) speichern möchten.
4. Geben Sie einen Namen für die Abfrage ein.
5. Klicken Sie auf **Speichern**, um die Abfrage zu exportieren.

Verwenden von Directory Manager für die Abfrage von Verzeichnissen über LDAP

Management Suite bietet neben einer Möglichkeit zur Abfrage der Core-Datenbank auch das Tool Directory Manager, mit dem Sie über LDAP (Lightweight Directory Access Protocol) auf Clients in Verzeichnissen zugreifen und verwalten können.

Sie können Clients basierend auf Attributen wie Prozessortyp oder Betriebssystem abfragen. Die Abfrage kann auch auf bestimmten Benutzerattributen wie Personalnummer oder Abteilung basieren.

Informationen zum Directory Manager-Fenster

Mit Directory Manager können Sie die folgenden Aufgaben ausführen:

- **Verzeichnis verwalten:** Öffnet das Dialogfeld "Verzeichniseigenschaften", in dem Sie ein LDAP-Verzeichnis angeben und anmelden können.
- **Verzeichnis entfernen:** Entfernt das ausgewählte Verzeichnis aus dem Vorschaufenster und beendet dessen Verwaltung.
- **Ansicht aktualisieren:** Lädt die Liste verwalteter Verzeichnisse und Zielbenutzer neu.
- **Neue Abfrage:** Öffnet das Dialogfeld LDAP-Abfrage, in dem Sie eine LDAP-Abfrage erstellen und speichern können.
- **Abfrage löschen:** Löscht die ausgewählte Abfrage.
- **Abfrage ausführen:** Erzeugt die Ergebnisse der ausgewählten Abfrage.
- **Objekteigenschaften:**Zeigt die Eigenschaften des ausgewählten Objekts an.
- **Application Policy Manager (APM):** Ruft das APM-Tool auf, sodass Sie Richtlinien für gespeicherte Abfragen oder einzelne LDAP-Benutzer bestimmen können.

Mit Directory Manager können Sie gespeicherte Abfragen und einzelne LDAP-Benutzer zum Application Policy Manager (APM) hinzufügen, um Richtlinien für diese zu bestimmen, Abfragen mit Ziehen und Ablegen als Zielliste in APM abzulegen und Benutzer auf eine statische Zielliste in APM zu verschieben.

Das Directory Manager-Fenster besteht aus zwei Bereichen: einem Verzeichnisbereich auf der linken Seite und einem Vorschaubereich auf der rechten Seite.

Verzeichnisbereich

Der Verzeichnisbereich zeigt alle registrierten Verzeichnisse und Benutzer. Als Administrator können Sie den Namen eines registrierten Verzeichnisses angeben und erhalten eine Liste der Abfragen, die mit diesem Verzeichnis verknüpft sind. Sie können mithilfe eines Rechtsklicks oder der Dropdown-Menüs neue Abfragen für ein registriertes Verzeichnis erstellen und speichern. Nach der Erstellung einer Abfrage können Sie sie mit Ziehen und Ablegen in den Application Policy Manager (APM) verschieben, sodass die Richtlinie auf Benutzer angewendet wird, die der Abfrage entsprechen.

Vorschaubereich

Wenn Sie eines gespeicherte Abfrage im Verzeichnisbereich des Directory Managers auf der linken Seite des Dialogfeldes auswählen, werden die für diese Abfrage bestimmten Richtlinien im Vorschaubereich auf der rechten Seite angezeigt. Wenn ein einzelner LDAP-Benutzer im Verzeichnisbereich ausgewählt wird, werden die Richtlinien, die für diesen Benutzer bestimmt sind, im Vorschaubereich angezeigt.

- **Registriertes Verzeichnis:**Abfragegruppenelement und Suchelement.
- **Abfragegruppen:** Mit dem Verzeichnis verknüpfte Abfragen.
- **Abfrage:** Liefert Details zur Abfrage.
- **Such- und Verzeichniselemente:** Unterelemente im Verzeichnis.
- **Alle Benutzer:** Führt alle Benutzer auf, für die derzeit Richtlinien bestimmt sind.
- **Einzelne Benutzer:** Führt die Richtlinien auf, die zur Zeit mit dem Benutzer verknüpft sind.

Erstellen von LDAP-Verzeichnisabfragen

So erstellen und speichern Sie eine Verzeichnisabfrage

Die Aufgabe der Erstellung einer Verzeichnisabfrage und des Speicherns dieser Abfrage gliedert sich in zwei Schritte:

So wählen Sie ein Objekt im LDAP-Verzeichnis aus und initiieren eine neue Abfrage

1. Klicken Sie auf **Extras | Directory Manager**.
2. Durchsuchen Sie den Verzeichnisbereich **Directory Manager** und wählen Sie ein Objekt im LDAP-Verzeichnis aus. Sie erstellen damit eine LDAP-Abfrage, die Ergebnisse von diesem Punkt ausgehend nach unten im Verzeichnisbaum ausgibt.
3. Klicken Sie im Directory Manager auf die Symbolleistenschaltfläche **Neue Abfrage**. Beachten Sie, dass dieses Symbol nur angezeigt wird, wenn Sie die Stammorganisation (o) des Verzeichnisbaums (o=mein Unternehmen) oder eine Organisationseinheit (ou=Engineering) innerhalb der Stammorganisation auswählen. Andernfalls ist es ausgeblendet.
4. Das Dialogfeld "Einfache LDAP-Abfrage" wird angezeigt.

So erstellen, testen und speichern Sie die Abfrage

1. Klicken Sie im Dialogfeld "Einfache LDAP-Abfrage" auf ein Attribut, das ein Kriterium für die Abfrage aus der Liste der Verzeichnisattribute sein soll (Beispiel = Abteilung).
2. Klicken Sie auf einen Vergleichsoperator für die Abfrage (=,<=, >=).
3. Geben Sie einen Wert für das Attribut ein (Beispiel Abteilung = Engineering).
4. Um eine komplexe Abfrage mit mehreren Attributen zu erstellen, wählen Sie einen Kombinationsoperator (AND oder OR) und wiederholen Schritte 1 bis 3 so oft wie nötig.
5. Wenn Sie die Erstellung der Abfrage beendet haben, klicken Sie auf **Einfügen**.
6. Zum Testen der fertiggestellten Abfrage klicken Sie auf **Abfrage testen**.

7. Zum Speichern der Abfrage klicken Sie auf **Speichern**. Die gespeicherte Abfrage erscheint mit ihrem Namen unter "Gespeicherte Abfragen" im Verzeichnisbereich des Directory Manager.

Informationen zum Dialogfeld "Einfache LDAP-Abfrage"

- **LDAP-Abfrageroot:** Wählen Sie ein Rootobjekt im Verzeichnis für diese Abfrage (LDAP://ldap.xyzunternehmen.com/ou = Amerika.o = xyzunternehmen). Die von Ihnen erstellte Abfrage gibt von diesem Punkt ausgehend nach unten im Baum Ergebnisse aus.
- **LDAP-Attribute:** Wählen Sie Attribute für Benutzerobjekte aus.
- **Operator:** Wählen Sie die Art des auszuführenden Vorgangs in Bezug auf ein LDAP-Objekt, dessen Attribute und Attributwerte einschließlich ist gleich (=), kleiner/gleich (<=) und größer/gleich (>=).
- **Wert:** Geben Sie den Wert an, der dem Attribut eines LDAP-Objekts zugewiesen ist.
- **Abfrage testen:** Führt einen Test der erstellten Abfrage durch.
- **Gespeichert:** Speichert die erstellte Abfrage nach Namen.
- **Erweitert:** Erstellt eine Abfrage mit den Elementen einer einfachen LDAP-Abfrage aber in freier Form.
- **Einfügen:** Fügt eine Zeile Abfragekriterien ein:
- **Löschen:** Löscht eine ausgewählte Kriterienzeile.
- **Alle löschen:** Löscht alle Zeilen mit Abfragekriterien.
- **Einfügen:** Fügt eine Zeile Abfragekriterien ein:

Informationen zum Dialogfeld "LDAP-Abfrage speichern"

Klicken Sie im Dialogfeld "Einfache LDAP-Abfrage" auf **Speichern**, um das Dialogfeld "LDAP-Abfrage speichern" zu öffnen, in dem Folgendes angezeigt wird:

- **Einen Namen für diese Abfrage wählen:** Ermöglicht Ihnen die Wahl eines Namens für die erstellte Abfrage.
- **Abfragedetails | LDAP-Root:** Hiermit können Sie eine Abfrage unter Verwendung der Elemente einer einfachen LDAP-Abfrage, jedoch in einem freien Format erstellen.
- **Abfragedetails | LDAP-Abfrage:** Zeigt Abfragebeispiele, die Sie als Richtlinie verwenden können, wenn Sie Ihre eigene Abfrage in freier Form erstellen.
- **Speichern:** Ermöglicht Ihnen, die erstellte Abfrage nach Namen zu speichern. Die Abfrage wird unter dem Punkt "Gespeicherte Abfragen" des LDAP-Verzeichniseintrags im Verzeichnisbereich Directory Manager gespeichert.

Nach dem Speichern einer Abfrage können Sie sie mit Ziehen und Ablegen in den Application Policy Manager (APM) verschieben, sodass sie auf Benutzer angewendet wird, die der Abfrage entsprechen.

Informationen zum Dialogfeld "Verzeichniseigenschaften"

Klicken Sie in der Symbolleiste Directory Manager auf die Symbolleistenschaltfläche **Verzeichnis verwalten**, um das Dialogfeld "Verzeichniseigenschaften" zu öffnen. Dieses Dialogfeld ermöglicht Ihnen die Verwaltung eines neuen Verzeichnisses oder die Anzeige der Eigenschaften eines derzeit verwalteten Verzeichnisses. Dieses Dialogfeld zeigt auch den URL zum LDAP-Server und die Authentifizierungsdaten, die für die Verbindung mit dem LDAP-Verzeichnis erforderlich sind.

- **Verzeichnis-URL:** Ermöglicht Ihnen die Angabe des zu verwaltenden LDAP-Verzeichnisses. Beispiel eines LDAP-Verzeichnisses mit korrekter Syntax: ldap.<firmenname>.com. Sie können beispielsweise ldap.xyzunternehmen.com eingeben.
- **Authentifizierung:**Damit können Sie:
  - Anmeldung als aktueller Benutzer (d. h. als Benutzer, der aktuell angemeldet ist).
  - Anmeldung als folgender Benutzer (d. h. Sie geben einen Benutzerpfad, einen Namen und ein Benutzerkennwort an).

Informationen zum Dialogfeld "Erweiterte LDAP-Abfrage"

Klicken Sie im Dialogfeld "Einfache LDAP-Abfrage" auf **Erweitert**, um das Dialogfeld "Erweiterte LDAP-Abfrage" zu öffnen, in dem Folgendes angezeigt wird:

- **LDAP-Abfrageroot:**Hiermit können Sie ein Root-Objekt für diese Abfrage auswählen. Die von Ihnen erstellte Abfrage gibt von diesem Punkt ausgehend nach unten im Baum Ergebnisse aus.
- **LDAP-Abfrage:** Hiermit können Sie eine Abfrage unter Verwendung der Elemente einer einfachen LDAP-Abfrage, jedoch in einem freien Format erstellen.
- **Beispiele:** Zeigt Abfragebeispiele, die Sie als Richtlinie verwenden können, wenn Sie Ihre eigene Abfrage in freier Form erstellen.
- **Abfrage testen:** Hiermit können Sie die Abfrage testen, die Sie erstellt haben.

Das Dialogfeld "Erweiterte LDAP-Abfrage" wird angezeigt, wenn Sie eine bereits erstellte Abfrage bearbeiten möchten. Wenn Sie eine LDAP-Gruppe im Directory Manager auswählen und davon ausgehend eine Abfrage erstellen möchten, wird das Dialogfeld "Erweiterte LDAP-Abfrage" mit einer Standardabfrage angezeigt, welche die Benutzer ausgibt, die der Gruppe angehören. Sie können die Syntax dieser Standardabfrage nicht ändern, sondern lediglich die Abfrage speichern.

Informationen über Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) ist ein dem Industriestandard entsprechendes Protokoll für den Zugriff auf und die Anzeige von Informationen über Benutzer und Clients. LDAP ermöglicht Ihnen die Organisation und Speicherung dieser Informationen in einem Verzeichnis. Ein LDAP-Verzeichnis ist insofern dynamisch, als dass es ggf. aktualisiert werden kann. Es wird verteilt, wodurch ein Schutz vor einem zentralen Ausfall gegeben ist. Zu allgemeinen LDAP-Verzeichnissen gehören Novell Directory Services* (NDS) und Microsoft Active Directory Services* (ADS).

Die folgenden Beispiele zeigen LDAP-Abfragen, die zum Durchsuchen des Verzeichnisses verwendet werden können:

- Alle Einträge abrufen: (objectClass=*)
- Einträge abrufen, die 'bob' an irgendeiner Stelle des Namens enthalten: (cn=*bob*)
- Einträge mit einem allgemeinen Namen abrufen, die größer/gleich 'bob' sind: (cn>='bob')
- Alle Benutzer mit einem E-Mail-Attribut abrufen: (&(objectClass=user)(email=*))
- Alle Benutzereinträge mit einem E-Mail-Attribut und einem Nachnamen abrufen, der 'smith' entspricht: (&(sn=smith)(objectClass=user)(email=*))
- Alle Benutzereinträge mit einem Namen abrufen, der mit 'andy', 'steve' oder 'margaret' beginnt: (&(objectClass=User) (|(cn=andy*)(cn=steve*)(cn=margaret*)))
- Alle Benutzer ohne E-Mail-Attribut abrufen: (!(email=*))

Die formale Definition des Suchfilters ist wie folgt (von RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> | <or> | <not> | <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> | <filter> <filterlist>
- <item> ::= <simple> | <present> | <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> | <approx> | <ge> | <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL | <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL | <value> '*' <starval>
- <final> ::= NULL | <value>

Der Token <attr> ist eine Zeichenfolge, die einen Attributtyp repräsentiert. Der Token <value> ist eine Zeichenfolge, die einen Attributwert repräsentiert, dessen Format vom zugrunde liegenden Verzeichnisdienst definiert wird.

Wenn ein <value> eines der folgenden Zeichen * oder (or) enthalten muss, stellen sie vor das Zeichen den Backslash (\).

Kapitel 4: Verwalten von Inventar und Berichten

LANDesk Management Suite verwendet einen Inventarscanner, um der Core-Datenbank Clients hinzuzufügen und Informationen zur Hard- und Software des Clients zu erfassen. Sie können Inventardaten anzeigen, drucken und exportieren. Des Weiteren können Sie Abfragen definieren, Clients gruppieren und besondere Berichte generieren.

In diesem Kapitel erfahren Sie mehr über:

Inventar

- Übersicht über das Inventarscannen
- Anzeigen von Inventardaten
- Verfolgen von Inventaränderungen
- Verwenden von benutzerdefinierten Datenformularen

Berichte

- Übersicht über Berichte
- Berichtsgruppen und vordefinierte Berichtslisten
- Erstellen von benutzerdefinierten Inventarberichten
- Ausführen von Berichten
- Verwenden der Berichtsansicht
- Importieren und Exportieren von Berichten

Hinweis: Weitere Informationen zum Ausführen des Inventarscanners sowie Tipps zur Fehlerbehebung beim Inventarscanner finden Sie in "Anhang A: Weitere Inventarvorgänge und Fehlerbehebung."

Übersicht über das Inventarscannen

Wenn Sie einen Client mit dem Client-Setup-Assistenten in Management Suite konfigurieren, können Sie eine Komponente "Inventarscanner" (einer der Management Suite-Agenten) auf dem Client installieren. Diese Komponente wird standardmäßig ausgewählt. Sie können den Inventarscanner auch in den Startordner des Clients einfügen, damit er immer beim Starten des Clients ausgeführt wird.

Der Inventarscanner wird automatisch beim ersten Konfigurieren des Clients ausgeführt. Die ausführbare Datei des Scanners heißt LDISCAN32.EXE und unterstützt Windows 95/98- und Windows NT/2000/XP-Clients. Der Inventarscanner erfasst Hard- und Softwaredaten und fügt sie in die Core-Datenbank ein. Danach wird der Hardwarescan immer beim Starten des Clients ausgeführt. Der Softwarescan wird dagegen nur in einem von Ihnen festgelegten Intervall ausgeführt. Um einen Softwarescan zu planen, klicken Sie auf **Konfigurieren | Dienste | Inventar | Prüfeinstellungen**.

Weitere Informationen zum Konfigurieren des Inventardienstes finden Sie unter "Konfigurieren des Inventardienstes" in Kapitel 1.

Nach dem ersten Scan kann der Inventarscanner manuell vom Client aus oder über die Management Suite-Konsole als geplante Task ausgeführt werden. Der CBA muss auf Fernclients ausgeführt werden, damit ein Inventarscan auf ihnen möglich ist.

Hinweis: Ein Client, der über die Erkennungsfunktion zur Core-Datenbank hinzugefügt wurde, hat seine Inventardaten noch nicht in die Core-Datenbank gescannt. Sie müssen einen Inventarscan auf jedem Client ausführen, damit die vollständigen Inventardaten für diesen Client angezeigt werden.

Sie können Inventardaten anzeigen lassen und damit:

- die Spalten der Netzwerkansicht anpassen, um bestimmte Inventarattribute anzuzeigen
- die Core-Datenbank nach Clients mit bestimmten Inventarattributen abfragen
- Clients gruppieren, um Verwaltungstasks wie die Softwaredistribution zu beschleunigen
- spezielle Berichte basierend auf Inventarattributen generieren

Mithilfe von Inventarscans können Sie auch Hardware- und Softwareänderungen auf Clients verfolgen und Warnungen oder Protokolldateieinträge generieren, wenn solche Änderungen auftreten. Weitere Informationen finden Sie unter "Verfolgen von Inventaränderungen" weiter unten in diesem Kapitel.

In den folgenden Abschnitten erfahren Sie mehr über die Funktionsweise des Inventarscanners.

Abstandsscannen

Nach dem ersten vollständigen Scan auf einem Client erfasst der Inventarscanner nur Abstandsänderungen und sendet diese an die Core-Datenbank. Somit wird das tägliche MODE=ALL in die Praxis umgesetzt. MODE=ALL sucht nach der gesamten auf dem Client installierten Software, einschließlich nicht erkannter Softwaredateien.

Hinweis: Weitere Informationen zum Softwarescannen und zu MODE=ALL finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE" in Kapitel 8 "Überwachen der Einhaltung von Softwarelizenzbestimmungen".

Erzwingen eines vollständigen Scans

Wenn Sie einen vollständigen Scan der Hard- und Softwaredaten eines Clients erzwingen möchten, verwenden Sie eine der folgenden Methoden:

- Löschen Sie die Datei INVDELTA.DAT vom Client. Eine Kopie des letzten Inventarscans ist lokal als verborgene Datei mit dem Namen INVDELTA.DAT im Stammverzeichnis des Laufwerks gespeichert. (Die Umgebungsvariable LDMS_LOCAL_DIR legt den Pfad dieser Datei fest.)
- Fügen Sie die Option **/sync** in die Befehlszeile des Inventarscanners ein. Um die Befehlszeile zu bearbeiten, klicken Sie mit der rechten Maustaste auf das Symbol **Inventarscan**, wählen **Eigenschaften** | **Kurzbefehl** und bearbeiten den Pfad **Ziel**.
- Setzen Sie den Registrierungsschlüssel "Do Delta" auf dem Core Server auf 0. Sie finden diesen Schlüssel unter : HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Do Delta

Scankomprimierung

Inventarscans mit dem Windows-Inventarscanner (LDISCAN32.EXE) werden standardmäßig komprimiert. Der Scanner komprimiert vollständige und Abstandsscans in einem Komprimierungsverhältnis von ca. 8:1. Scans werden zunächst vollständig im Speicher erstellt, dann komprimiert und mithilfe eines größeren Pakets an den Core Server gesendet. Die Scankomprimierung reduziert die Anzahl der erforderlichen Pakete und die Bandbreitennutzung.

Scanverschlüsselung

Inventarscans werden nun verschlüsselt (nur TCP/IP-Scans).

Sie können die Verschlüsselung von Inventarscans deaktivieren, indem Sie den Registrierungsschlüssel "Disable Encryption" auf dem Core Server auf 0 setzen. Dieser Schlüssel befindet sich unter:
HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Disable Encryption

Anzeigen von Inventardaten

Sobald ein Client vom Inventarscanner gescannt wurde, können Sie seine Systeminformationen in der Management Suite-Konsole ansehen.

Clientinventare werden in der Core-Datenbank gespeichert. Sie umfassen Hardware-, Gerätetreiber-, Software-, Speicher- und Umgebungsinformationen. Die Inventarinformationen sind beim Verwalten und Konfigurieren von Clients hilfreich. Außerdem können Sie damit schnell Systemprobleme erkennen.

Inventardaten können folgendermaßen angezeigt werden:

- Inventarübersicht
- Vollständiges Inventar

Darüber hinaus können Inventardaten auch in von Ihnen generierten Berichten angezeigt werden. Weitere Informationen finden Sie unter "Übersicht über Berichte" weiter unten in diesem Kapitel.

Anzeigen einer Inventarübersicht

Eine Inventarübersicht finden Sie auf der Eigenschaftenseite des Clients. Sie bietet eine schnelle Übersicht über die Betriebssystemkonfiguration sowie Systeminformationen des Clients. Die Übersicht zeigt außerdem Datum und Uhrzeit des letzten Inventarscans, damit Sie wissen, wie aktuell die Daten sind.

Hinweis: Wenn Sie einen Client mithilfe des Erkennungswerkzeugs in die Core-Datenbank eingefügt haben, sind seine Inventardaten noch nicht in die Core-Datenbank gescannt. Sie müssen einen Inventarscan auf dem Client ausführen, damit die Inventarübersicht erfolgreich erstellt werden kann.

So zeigen Sie eine Inventarübersicht an

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf einen Client.
2. Klicken Sie auf **Eigenschaften** | Registerkarte **Inventar**.

Die Inventarübersicht ist bei Windows NT/2000- und Windows 9.x/ME-Clients unterschiedlich. In den folgenden Listen werden die verschiedenen Datenkomponenten nach Betriebssystem angezeigt.

Daten eines Windows NT/2000-Clients

Diese Informationen werden angezeigt, wenn Sie die Inventarübersicht für einen Windows NT/2000/XP-Client anzeigen.

NT-Konfiguration:

- **Computername:** Der dem Client zugewiesene NetBIOS-Name.
- **Domänenname:** Domäne, in der sich der Client befindet.

- **Betriebssystem:** Windows-Betriebssytem, das auf dem Client ausgeführt wird: NT, 2000 oder XP.
- **Version:** Versionsnummer des Windows NT/2000/XP-Betriebssystems, das auf dem Client ausgeführt wird.
- **Build:** Buildnummer der Windows NT/2000/XP-Software. Diese Nummer präzisiert die Version, die auf dem Client ausgeführt wird.

System

- **Prozessortyp:** Prozessor(en), der bzw. die auf dem Client ausgeführt werden.
- **Prozessorgeschwindigkeit:** Geschwindigkeit der CPU(s).
- **Prozessoranzahl:** Anzahl der Prozessoren im Client.
- **Math-Koprozessor:** Typ des Math-Koprozessors, sofern vorhanden. Mögliche Werte sind "Intern" oder "Extern".
- **Bustyp:** Bustyp des Windows NT/2000/XP-Clients. In diesem Feld können vier Bustypen angezeigt werden: Industry Standard Architecture (ISA), Micro Channel Architecture (MCA), Extended Industry Standard Architecture (EISA) und Peripheral Component Interface (PCI).
- **BIOS-Datum:** Datum der ROM-BIOS-Version.
- **Physischer Speicher:** Auf dem Client verfügbarer RAM.
- **Virtueller Speicher:** Auf dem Client verfügbarer Speicher, einschließlich RAM und Speicher der Auslagerungsdatei.

Daten eines Windows 9.x/ME-Clients

Hardware:

- **Rechnertyp:** Zu den unterstützten Clients (Rechnern) gehören PC/AT, PC/XT und PS/2. Der richtige Rechnertyp wird nur für IBM-Clients zurückgegeben. IBM-kompatible Rechner werden normalerweise als der IBM-Typ angezeigt, dem sie am ehesten entsprechen. Wenn Management Suite das Modell nicht erkennen kann, werden Modell- und Untermodellnummern angezeigt.
- **CPU-Typ:** Management Suite erkennt neben gängigen Intel-kompatiblen Prozessoren von Drittanbietern auch 80386- und größere Prozessoren.
- **CPU-Taktfrequenz:** Taktfrequenz des Prozessors in MHz.
- **Math-Koprozessor:** Typ des Math-Koprozessors, sofern vorhanden. Mögliche Werte sind "Intern" oder "Extern".
- **Bustyp:** Management Suite erkennt folgende Bustypen: Industry Standard Architecture (ISA), MicroChannel Architecture* (MCA), Extended Industry Standard Architecture (EISA) und Peripheral Component Interface (PCI).
- **Videoadapter:** Management Suite erkennt folgende Adaptertypen: Monochrom, VGA Farbe und VGA Monochrom. Diese Information stammt vom CMOS. Wenn Management Suite den Videoadapter nicht erkennt, wird im Normalfall "Monochrom" angegeben.

Speicher:

- **Konventionell:** Größe des konventionellen Speichers. Konventioneller Speicher ist der Speicher, auf den DOS für seine Verarbeitungstasks direkt zugreift. Jeder DOS-basierte Client besitzt 640 KB konventionellen Speicher.

- **Erweiterungsspeicher:** Größe des Erweiterungsspeichers (XMS). Erweiterungsspeicher ist der Hauptspeicher über 1 MB, der nicht als Expansionsspeicher konfiguriert wurde.
- **Expansionsspeicher** Größe des Expansionsspeichers (EMS). Expansionsspeicher ist Speicher über 1 MB, der nur von Anwendungen verwendet werden kann, die eine der Expansionsspeicher-Spezifikationen unterstützen.
- **Basis:** Basisadresse (in Hexadezimaldarstellung) des Speicherbereichs, der vom EMS reserviert wurde, soweit vorhanden. Die Größe dieses Bereichs und seine Anfangsadresse hängen vom installierten EMS-Treibertyp, von der Größe des installierten Expansionsspeichers und von den anderen im konventionellen Speicher geladenen Programmen ab.

Umgebung:

- **Mausunterstützung** Der auf dem Client installierte Maustreiber. Unterstützte Typen sind: seriell; Bus, Inport*, PS/2 und Hewlett Packard.
- **BIOS-Datum:** Datum der ROM-BIOS-Version.
- **DOS-Version:** Version des verwendeten DOS.
- **Ports:** Im Gruppenfeld "Drucker-Ports" werden die Adressen aller seriellen und parallelen Ports des Clients angezeigt.

Anzeigen eines vollständigen Inventars

Ein vollständiges Inventar umfasst eine komplette und ausführliche Aufstellung der Hardware- und Softwarekomponenten eines Clients. Die Aufstellung enthält Objekte und Objektattribute.

So zeigen Sie ein vollständiges Inventar an

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf einen **Client**.
2. Klicken Sie auf **Inventar**.

Informationen zum Fenster "Inventar"

Im Fenster "Inventar" können Sie das komplette Inventar eines Clients anzeigen, einschließlich folgender Komponenten:

- **BIOS:** Typ, Datum, ID-Byte und Systemmodell des BIOS. Das BIOS befindet sich permanent im ROM (Read-Only Memory, schreibgeschützter Speicher) des Computers und ermöglicht die Kommunikation zwischen Speicher, Festplattenlaufwerken und Bildschirm.

Weitere BIOS-Informationen werden im Fenster "Inventar" als BIOS-Textzeichenfolgen angezeigt. Um BIOS-Textzeichenfolgen anzuzeigen und zu suchen, erweitern Sie das Objekt **BIOS**, wählen Sie **BIOS-Zeichenfolgen**, klicken Sie mit der rechten Maustaste auf das Attribut **Daten** und wählen Sie **Eigenschaften**; klicken Sie anschließend auf **Erweiterter Wert**. Während eines Inventarscans gibt Management Suite die im BIOS verfügbaren Textzeichenfolgen in die Textdatei LDBIOS.TXT aus. Sie können eine Abfrage in der Datei LDAPPL3.INI einrichten, mit der eine oder mehrere der BIOS-Textzeichenfolgen an die Konsole ausgegeben werden. Weitere Informationen finden Sie in "Anhang A: Weitere Inventarvorgänge und Fehlerbehebung".

- **Bus:** Bustyp. Der Bus verbindet den Mikroprozessor, Festplattenlaufwerke, Speicher und Eingabe-/Ausgabe-Ports miteinander. Mögliche Bustypen sind: ISA, EISA, VESA Lokaler Bus, PCI und USB.
- **Koprozessor:** Typ des Koprozessors, sofern vorhanden. Der Koprozessor ist nicht identisch mit dem Hauptmikroprozessor, obwohl er sich auf demselben Motherboard oder sogar demselben Chip befinden kann. Der Math-Koprozessor evaluiert den Gleitkommabetrieb für den Hauptmikroprozessor.
- **Umgebung:** Speicherorte, Befehlspfade, Systemeingabeaufforderungen und andere Variablen für die Windows-Umgebung.
- **Tastatur:** Die an den Client angeschlossene Tastatur. Derzeit ist die erweiterte IBM-Tastatur die gebräuchlichste Tastatur. Die Tastatur verwendet Codeseiten.
- **LANDesk Management:** Information zu LANDesk-Agenten, LANDesk Client Manager und Alert Management System (AMS). Enthält auch Informationen zum Inventarscanner und zu Initialisierungsdateien.
- **Massenspeicher:** Speichergeräte auf dem Computer, einschließlich Disketten, Festplatten, logische und Bandlaufwerke sowie CD-ROM. Die Festplatten- und Diskettenlaufwerkobjekte umfassen Attribute für Kopf, Nummer, Sektor und Gesamtspeicherkapazität.
- **Speicher:** Attribute für Auslagerungsdatei, physischen und virtuellen Speicher. Jedes dieser Speicherobjekte enthält Byte-Attribute. Das erste Byte ist die Größe des verfügbaren Speichers. Das zweite Byte ist die Gesamtspeicherkapazität.
- **Maus:** Die an den Client angeschlossene Maus. Mögliche Maustypen sind u. a.: PS/2, seriell und Infrarot.
- **Netzwerk:** Netzwerkadapter, NIC-Adresse und Knotenadresse der Adapter. Das Netzwerkobjekt enthält Informationen für jedes auf dem Computer geladene Protokoll. Typische Werte sind IPX*-, NetBEUI-, NetBIOS- und TCP/IP-Objekte.

    - **IPX** ist ein Protokoll, das NetWare*-Server zur Kommunikation mit ihren Clients und anderen Servern verwenden. Das IPX-Objekt enthält die Attribute für Adresse, Netzwerknummer und Knotenadresse.
    - **NetBEUI** ermöglicht einem Computer die Kommunikation mit Windows NT/2000-, Windows für Workgroups- oder LAN Manager-Servern. Microsoft empfiehlt nun die Verwendung von TCP/IP für diese Verbindungen.
    - **NetBIOS** ist eine Schnittstelle (API), über die Anwendungen sich gegenseitig Pakete über TCP/IP, NetBEUI oder IPX senden bzw. empfangen können.

- **TCP/IP** ist ein Protokoll, mit dem ein Computer über das Internet und mit WANs kommunizieren kann. Dieses Objekt enthält die Adresse (enthält die TCP/IP-Adresse des Computers), den Hostnamen (enthält den DNS-Kontext des Computers), aktiviertes IP-Routing und die NetBIOS-Auflösung (verwendet die Attribute "DNS-Proxy aktiviert" und "WINS-Proxy aktiviert").

- **Netzwerkadapter:** Attribute für jeden auf dem Client installierten Netzwerkadapter.
- **Betriebssystem:** Betriebssystem, Treiber, Dienste und Ports. Diese Objekte und ihre Attribute variieren je nach den Konfigurationen der geladenen Treiber und Dienste.
- **Ports:** Objekte für jeden Ausgabe-Port des Computers (seriell und parallel). Jeder Ausgabe-Port enthält Adress- und Namensattribute. Das Adressattribut enthält die Hardwareadresse für den Port.
- **Drucker:** Objekte für jeden Drucker, der direkt oder über ein Netzwerk an den Computer angeschlossen ist. Die Druckerobjekte enthalten Treiber-, Namens-, Nummern- und Port-Attribute. Das Port-Attribut enthält entweder die Netzwerkwarteschlange oder den Port, an den der Drucker angeschlossen ist.
- **Prozessor:** Attribute der Client CPU. Erkennt Intel-, Motorola 680x0- und PowerPC-Prozessoren.
- **Ressourcen:** Objekte für jede Hardwareressource des Computers. Jedes Objekt einer Hardwareressource enthält Attribute, die den Ressourcentyp und alle von ihm verwendeten Ports und Interrupts beschreiben.
- **Software:** Objekte für jede auf der Festplatte des Clients installierte Softwareanwendung. Jedes Objekt eines Softwareprogramms listet Attribute auf, die typischerweise den Namen, den Speicherort und die Versionsnummer der Software enthalten.
- **Video:** Objekte für jeden Videoadapter des Clients. Das Videoadapterobjekt enthält im Normalfall Attribute, die die Auflösung und die Anzahl der unterstützten Farben beschreiben.

Anzeigen von Attributeigenschaften

In der Inventarliste können Sie Attributeigenschaften für die Inventarobjekte eines Clients anzeigen. Attributeigenschaften geben Aufschluss über die Eigenschaften und Werte eines Inventarobjekts. Sie können auch neue, angepasste Attribute erstellen und benutzerdefinierte Attribute bearbeiten.

Um die Eigenschaften eines Attributs anzuzeigen, doppelklicken Sie auf das Attribut.

Informationen zum Dialogfeld "Inventarattributeigenschaften"

In diesem Dialogfeld können Sie die Eigenschaften eines Attributs anzeigen. Die Registerkarte "Merkmale" enthält folgende Informationen:

- **Name:** Der Name des Core-Datenbank-Attributs, dessen Eigenschaften angezeigt werden.
- **Wert:** Der diesem Inventarattribut zugewiesene Wert.
- **Benutzerdefiniert:** Gibt an, ob das ausgewählte Attribut vom Benutzer definiert wurde. Diese Option kann nicht geändert werden.

- **Primärschlüssel:** Gibt an, ob das Attribut Objekte desselben Typs eindeutig identifiziert. Ein Objekt kann nur einen Primärschlüssel besitzen.
- **Ereignisprotokoll bei Änderung benachrichtigen:** Gibt an, ob eine Änderung dieses Attributs im Windows-Ereignisprotokoll erfasst werden soll.
- **Änderungen in Datenbankverlauf verfolgen:** Gibt an, ob Änderungen dieses Attributs im Inventarverlaufsprotokoll erfasst werden sollen.
- **AMS-Alarm ausgeben:** Gibt an, ob Änderungen dieses Attributs an AMS gesendet werden sollen, damit ein Alarm ausgegeben wird.
- **Ereignisprotokoll/Alarmwichtigkeit:** Die Wichtigkeit eines Protokoll- oder Alarmeintrags.
- **Faktor (nur Ganzzahlenwerte):** Ganzzahlenwerte, mit denen das Attribut in Einheiten unterteilt wird. Wenn Sie den Faktorwert ändern, müssen Sie den entsprechenden Code im Feld "Formatbezeichner" eingeben. Wenn das Attribut in Kilobyte angegeben wurde und jetzt in Megabyte angezeigt werden soll, geben Sie den Wert "1000" ein.
- **Formatbezeichner (nur Ganzzahlenwerte):** Schreibweise, mit der der Wert in der richtigen Form angezeigt wird. Beispielsweise wird der Attributwert mit "%d MB" ohne Dezimalstellen angezeigt; mit "%.1f MB" wird der Attributwert bis zur ersten Gleitkommastelle in MB angezeigt. Wenn kein Faktor eingegeben wird, muss dieser Formatbezeichner Ganzzahlenwerte beschreiben (%d, %u usw.). Wenn ein Faktor eingegeben wird, muss dieser Formatbezeichner Gleitkommawerte beschreiben (%f, %e usw.).

Verfolgen von Inventaränderungen

Management Suite kann Änderungen an der Hard- und Software des Clients erkennen und erfassen. Wenn Sie Inventaränderungen verfolgen, haben Sie einen besseren Überblick über Ihren Netzwerkbestand. Mit den Inventaränderungseinstellungen können Sie auswählen, welche Arten von Änderungen mit welchem Wichtigkeitsgrad gespeichert werden sollen. Die ausgewählten Änderungen können in einem Inventarverlaufsprotokoll oder dem NT-Ereignisprotokoll des Core Servers gespeichert oder als AMS-Alarm gesendet werden.

Sie können den Verlauf der Inventaränderungen eines Clients anzeigen und drucken. Zusätzlich können Sie Inventaränderungen in eine .CSV-formatierte Datei für Analysen mit eigenen Berichterstellungstools exportieren.

Um Inventaränderungen zu verfolgen und zu nutzen, müssen Sie zuerst die Inventaränderungseinstellungen konfigurieren. Sie können die anderen Tasks in Bezug auf den Inventaränderungsverlauf ausführen:

- Konfigurieren von Inventaränderungseinstellungen
- Anzeigen, Drucken und Exportieren von Inventaränderungen

Konfigurieren von Inventaränderungseinstellungen

Hinweis: Sie müssen zuerst diese Einstellungen konfigurieren, wenn Sie Inventaränderungen für einen Client im Netzwerk anzeigen, drucken oder exportieren möchten.

So konfigurieren Sie Inventaränderungseinstellungen

1. Klicken Sie auf **Konfigurieren | Inventarverlauf**.
2. Erweitern Sie im Dialogfeld "Inventaränderungseinstellungen" das Objekt **Computer** in der Liste "Aktuelles Inventar", und wählen Sie anschließend die zu verfolgenden Systemkomponenten aus.
3. Wählen Sie in der Liste "Ereignis protokollieren in" das Attribut der Komponente aus, das verfolgt werden soll.
4. Aktivieren Sie das entsprechende Kontrollkästchen, um anzugeben, wo Änderungen dieses Attributs erfasst werden sollen. Inventaränderungen können im Protokoll der Inventaränderungsverlaufs, im Protokoll der Windows NT-Ereignisanzeige oder als AMS-Alarm aufgezeichnet werden.
5. Wählen Sie einen Wichtigkeitsgrad in der Dropdown-Liste "Protokoll/Alarmwichtigkeit" aus. Folgende Wichtigkeitsgrade stehen zur Auswahl: Keine, Informationen, Warnung und Kritisch.
6. Klicken Sie auf **OK**.

Informationen zum Dialogfeld "Inventaränderungseinstellungen"

Verwenden Sie dieses Dialogfeld, um auszuwählen, welche Inventarattribute protokolliert werden, wenn Änderungen an einzelnen Clients vorgenommen werden, und um anzugeben, wo diese Änderungen protokolliert werden.

- **Aktuelles Inventar:** Listet alle in der Core-Datenbank gespeicherten Objekte auf. Klicken Sie auf ein Objekt, um seine Attribute in der Liste "Ereignis protokollieren in" anzuzeigen. Erweitern Sie eine Objektgruppe, um die darin enthaltenen Datenobjekte anzuzeigen.
- **Ereignis protokollieren in:** Zeigt die Attribute des in der Liste "Aktuelles Inventar" ausgewählten Inventarobjekts.

  Um festzulegen, wo Inventaränderungen protokolliert werden, wählen Sie ein Attribut aus, und aktivieren Sie eine oder mehrere Optionen. Aktivieren Sie die Option **Inventar**, um Inventaränderungen im Dialogfeld "Inventaränderungsverlauf" zu protokollieren. Aktivieren Sie die Option **NT-Protokoll**, um Inventaränderungen im Windows NT-Ereignisprotokoll zu erfassen. Aktivieren Sie die Option **AMS**, um Inventaränderungen als Alarm über AMS zu senden. (AMS-Alarmmeldungen werden mit dem Tool "Alarmeinstellungen" konfiguriert.)

- **Protokoll/Alarmwichtigkeit:** Enthält die Optionen für die Alarmpriorität. Diese Funktion wird erst aktiviert, wenn ein Attribut ausgewählt ist. Sie können zwischen den Wichtigkeitsgraden "Keine", "Informationen", "Warnung" und "Kritisch" auswählen.

Anzeigen, Drucken und Exportieren von Inventaränderungen

So zeigen Sie Inventaränderungen an, drucken oder exportieren sie

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf einen oder mehrere Clients.
2. Klicken Sie auf **Inventarverlauf**.
3. Klicken Sie auf **Drucken**, um den Inventaränderungsverlauf zu drucken.
4. Klicken Sie auf **Exportieren**, um den Inventaränderungsverlauf als .CSV-Datei zu speichern.

Informationen zum Dialogfeld "Inventaränderungsverlauf"

In diesem Dialogfeld können Sie die Inventaränderungen eines Clients anzeigen. Außerdem können Sie den Inventaränderungsverlauf in diesem Dialogfeld drucken und exportieren.

- **Gerätename:** Zeigt den Namen des bzw. der Clients an, die in der Netzwerkansicht der Konsole ausgewählt wurden und für die Inventaränderungsdaten angefordert wurden.
- **Komponente:** Gibt die geänderte Systemkomponente an. (Hier werden nur Komponenten angezeigt, die im Dialogfeld "Inventaränderungseinstellungen" ausgewählt wurden.)
- **Attribut:** Gibt an, welches Attribut der Komponente protokolliert wird.
- **Zeit:** Gibt an, wann die Änderung erfolgt ist.
- **Neuer Wert:** Zeigt den neuen (geänderten) Wert für das angegebene Attribut.
- **Alter Wert:** Zeigt den alten (vorherigen) Wert für das angegebene Attribut.

- **Drucken:** Öffnet ein Standardruckdialogfeld, in dem Sie den Inhalt des Inventaränderungsverlaufs drucken können.
- **Exportieren:** Öffnet ein Dialogfeld "Speichern unter", in dem Sie einen Namen und den Speicherort der exportieren .CSV-Datei mit dem Inventaränderungsverlauf auswählen können.

Sie können auf eine Spaltenüberschrift klicken, um die Liste nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Überschrift, um die Sortierreihenfolge wieder umzukehren.

Verwenden von benutzerdefinierten Datenformularen

Management Suite enthält ein Tool für benutzerdefinierte Datenformulare (**Extras | Benutzerdefinierte Datenformulare**), mit dem Sie Formulare erstellen und verwalten können. Mithilfe von benutzerdefinierten Datenformularen können Sie Informationen von Benutzern erfassen und in die Core-Datenbank einfügen.

Bestimmte benutzerspezifische Informationen können vom Inventarscanner nicht erfasst werden. Beispiele:

- Wo befindet sich der Schreibtisch eines Benutzers?
- Wie lautet die Inventarnummer eines Benutzers?
- Wie lautet die Telefonnummer eines Benutzers?

Diese Informationen erhalten Sie am besten mit benutzerdefinierten Datenformularen direkt von den Benutzern.

Benutzerdefinierte Datenformulare bestehen aus zwei Hauptkomponenten: dem Form Designer, mit dem Sie Formulare erstellen, die vom Benutzer ausgefüllt werden müssen, und der Formularanzeige, die Benutzer zum Ausfüllen von Formularen verwenden.

Formulare können zentral oder lokal gespeichert werden. Wenn sie zentral gespeichert werden, haben alle Benutzer automatisch Zugriff auf die neuesten Formulare, weil jeder dasselbe Formular am selben Speicherplatz sieht. Wenn Formulare lokal gespeichert werden, müssen Sie sicherstellen, dass Benutzer die neuesten Formulare erhalten.

Nachdem ein Benutzer ein Formular ausgefüllt hat, speichert die Formularanzeige die Ergebnisse lokal in der Datei \LDClient\LDCUSTOM.DAT. Diese Datei enthält die Ergebnisse aller Formulare, die der Benutzer ausgefüllt hat. Wenn der Benutzer dasselbe Formular noch einmal ausfüllen muss (z. B. wenn das Originalformular überarbeitet wurde), fügt die Formularanzeige automatisch die zuvor eingegebenen Daten ein.

Der Inventarscanner nimmt die Informationen aus der Datei LDCUSTOM.DAT jedes Clients und fügt sie der Core-Datenbank hinzu.

Bei Oracle-Datenbanken muss die Groß-/Kleinschreibung beachtet werden
Wenn Sie benutzerdefinierte Felder mit benutzerdefinierten Datenformularen (oder einer anderen Funktion in Management Suite) in einer Oracle-Datenbank erstellen, müssen Sie bei den Feldnamen auf die Groß-/Kleinschreibung achten. Daten von "Würfelspeicherort" werden an einer anderen Stelle in der Datenbank gespeichert als Daten von "WÜRFELSPEICHERORT".

Stellen Sie außerdem sicher, dass benutzerdefinierte Felder unabhängig von der Großschreibung eindeutige Namen besitzen. Management Suite ruft unter Umständen die falschen Inventardaten ab, wenn zwei benutzerdefinierte Felder denselben Namen mit unterschiedlicher Groß-/Kleinschreibung verwenden.

Weitere Informationen zu benutzerdefinierten Datenformularen finden Sie in den folgenden Schrittanweisungen:

- Erstellen eines benutzerdefinierten Datenformulars
- Erstellen einer Gruppe von Formularen
- Konfigurieren von Clients für den Empfang von benutzerdefinierten Datenformularen
- Ausfüllen von Formularen auf dem Client

Erstellen eines benutzerdefinierten Datenformulars

Führen Sie folgende Schritte aus, um ein benutzerdefiniertes Datenformular zu erstellen.

So erstellen Sie ein benutzerdefinierten Datenformular

1. Klicken Sie auf **Extras | Benutzerdefinierte Datenformulare**.
2. Doppelklicken Sie im Fenster "Benutzerdefinierte Datenformulare" auf **Neues Formular hinzufügen**.
3. Geben Sie einen Namen für das Formular ein.
4. Geben Sie eine Beschreibung für das Formular ein.
5. Klicken Sie auf **Hinzufügen**, um das Dialogfeld "Frage hinzufügen" zu öffnen.
6. Geben Sie im Dialogfeld "Frage hinzufügen" Text in die Felder **Fragetext**, **Inventarname** und **Beschreibung** ein.
7. Wählen Sie die **Steuerungsart** aus.
8. Geben Sie an, ob das Feld ein erforderliches Feld werden soll.
9. Wenn Sie die Steuerungsart **Bearbeitungsfeld** auswählen, klicken Sie auf **Beenden**, um das Dialogfeld "Frage hinzufügen" zu schließen. Mit der Steuerungsart "Bearbeitungsfeld" können Benutzer eigene Antworten in einem bearbeitbaren Textfeld eingeben. Sie können weitere Fragen hinzufügen oder bei Schritt 12 fortfahren.
10. Wenn Sie eine der Steuerungsarten **Kombinationsfeld** auswählen, klicken Sie auf **Weiter**, um das Dialogfeld "Elemente hinzufügen" zu öffnen. Mit der Steuerungsart "Kombinationsfeld" können Benutzer ihre Antworten in einer Dropdown-Liste mit vordefinierten Elementen auswählen.
11. Geben Sie im Dialogfeld "Elemente hinzufügen" einen Elementnamen ein, und klicken Sie auf **Einfügen**, um das Element in die Elementliste einzufügen. Diese Elemente werden in einer Dropdown-Liste für diese Frage auf dem Formular angezeigt. Sie können beliebig viele Elemente hinzufügen, bevor Sie auf **Beenden** klicken.
12. Wenn Sie keine weiteren Fragen hinzufügen möchten, klicken Sie auf **Schließen**, um das Formular zu speichern.

Wenn Sie mit der rechten Maustaste auf ein Formular klicken, können Sie seine Verteilung an Clients planen.

Informationen zum Dialogfeld "Benutzerdefiniertes Datenformular erstellen/bearbeiten"

In diesem Dialogfeld können Sie ein benutzerdefiniertes Datenformular erstellen oder bearbeiten.

- **Formularname:** Identifiziert das Formular und ist auf der Formularanzeige zu sehen, wenn ein Benutzer das Formular ausfüllt.
- **Beschreibung:** Stellt Benutzern zusätzliche Informationen zum Formular zur Verfügung.
- **Hinzufügen:** Öffnet das Dialogfeld "Frage hinzufügen", in dem Sie eine neue Frage für das Formular erstellen können.
- **Bearbeiten:** Öffnet das Dialogfeld "Frage bearbeiten", in dem Sie die Optionen einer beliebigen Frage bearbeiten können.
- **Löschen:** Entfernt die Frage vom Formular.
- **Seitenumbruch:** Steuert das Layout des Formulars, indem Seitenumbrüche zwischen zusammengehörigen Fragengruppen eingefügt werden. Bei einem Seitenumbruch müssen Benutzer auf "Weiter" klicken, um zu den Fragen auf der nächsten Seite zu gelangen.

  Hinweis: Eine Seite kann maximal neun Fragen enthalten.

- **Vorschau:** Öffnet das Formular, damit Sie vorab sehen können, wie das Formular für Benutzer angezeigt wird. Im Vorschaumodus müssen Sie keine Daten einfügen, und Ihre Eingaben werden nicht gespeichert.

Informationen zum Dialogfeld "Frage hinzufügen/bearbeiten"

In diesem Dialogfeld können Sie Fragen erstellen oder bearbeiten, die auf dem benutzerdefinierten Datenformular angezeigt werden. Formulare bestehen aus Fragen und freiem Platz, in dem Benutzer ihre Antworten eingeben können. Legen Sie zunächst die Frage fest:

- **Fragetext:** Einzeilige Beschreibung der Frage. Dieser Text wird neben dem Datenfeld angezeigt.
- **Inventarname:** Name des Datenbankfeldes in der Core-Datenbank. Wenn Sie die Core-Datenbank nach diesem Element abfragen möchten, erstellen Sie eine Abfrage nach der Bezeichnungs-ID.
- **Beschreibung:** Zusätzliche Informationen, die angezeigt werden, wenn Benutzer auf "Hilfe" klicken (oder F1 drücken), während sie sich im Datenfeld dieser Frage befinden.

Sie müssen auch angeben, welche Art von Datenfeld (Steuerung) neben jeder Frage angezeigt wird und ob es ein erforderliches Feld ist. Folgende Datenfelder stehen zur Verfügung:

- **Bearbeitungsfeld:** Benutzer geben ihre Antwort in einem bearbeitbaren Textfeld ein.
- **Kombinationsfeld (Bearbeitungsliste):** Benutzer wählen einen der vordefinierten Listeneinträge aus oder geben eine eigene Antwort ein.
- **Kombinationsfeld (feste Liste):** Benutzer wählen einen der vordefinierten Listeneinträge aus.
- **Steuerung ist erforderliches Feld und muss ausgefüllt werden:** Der Benutzer ist gezwungen, diese Frage zu beantworten. Der Benutzer kann das Formular erst beenden oder zur nächsten Seite wechseln, wenn er eine Antwort in die erforderlichen Felder eingegeben hat.

Informationen zum Dialogfeld "Elemente hinzufügen"

Verwenden Sie dieses Dialogfeld, um Elemente in eine Dropdown-Liste einzufügen, aus der ein Benutzer Antworten für diese Frage auf einem Formular auswählen kann.

- **Elementname:** Identifiziert das Element. Dieser Name wird in der Dropdown-Liste der Frage angezeigt.
- **Elementliste:** Enthält alle Elemente, die in der Dropdown-Liste der Frage angezeigt werden.
- **Einfügen:** Fügt das Element in die Elementliste ein.
- **Löschen:** Entfernt das Element von der Elementliste.

Erstellen einer Gruppe von Formularen

Wenn Sie mehr als ein Formular an Clients senden möchten, können Sie sie in Gruppen zusammenfassen. Dann können Sie problemlos die Verteilung der Formulargruppe planen. Dieser Vorgang ist natürlich nicht zwingend erforderlich.

Beim Planen der Verteilung einer Gruppe von Formularen liest "Geplante Tasks" den Inhalt der Gruppe, wenn der Zeitpunkt der Verteilung gekommen ist. Das bedeutet, Sie können den Inhalt der Gruppe auch dann noch ändern, wenn ihre Verteilung bereits geplant ist (solange der geplante Auftrag noch nicht ausgeführt wurde).

Hinweis: Wenn ein Formular der Gruppe später geändert oder gelöscht wird, spiegelt die Gruppe diese Änderungen sofort wider.

So erstellen Sie eine Gruppe von Formularen

1. Klicken Sie in der Symbolleiste des Fensters "Benutzerdefinierte Formulare" auf die Schaltfläche **Mehrere Formulare**.
2. Geben Sie einen Namen für die neue Gruppe ein.
3. Wählen Sie die Formulare, die der Gruppe hinzugefügt werden sollen, in der Liste der verfügbaren Formulare aus.
4. Klicken Sie auf **OK**.

Wenn Sie mit der rechten Maustaste auf eine Gruppe von Formularen klicken, können Sie ihre Verteilung an Clients planen.

Informationen zum Dialogfeld "Mehrere Formulare zur Verteilung auswählen"

In diesem Dialogfeld erstellen Sie eine Gruppe von Formularen. Es zeigt den Namen der Gruppe und alle verfügbaren Formulare, die Teil einer Gruppe sein können.

- **Name der neuen Gruppe:** Identifiziert die Gruppe im Fenster "Benutzerdefinierte Datenformulare".
- **Verfügbare Formulare:** Zeigt alle verfügbaren Formulare an, die der Gruppe hinzugefügt werden können.
- **OK:** Speichert die Gruppe und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Gruppe zu speichern.

Konfigurieren von Clients für den Empfang von benutzerdefinierten Datenformularen

Beim Einrichten von Clients können Sie sie so konfigurieren, dass sie benutzerdefinierte Datenformulare empfangen können. Sie müssen die Komponente "Benutzerdefinierte Datenformulare" installieren und Optionen auf den Seiten "Benutzerdefiniertes Formular" des Client-Setup-Assistenten festlegen. Weitere Informationen finden Sie unter "Verteilen benutzerdefinierter Datenformulare" in Kapitel 2.

Im Client-Setup-Assistenten müssen Sie festlegen, wie Formulare auf dem Client aktualisiert werden sollen:

- **Automatische Aktualisierung:** Wenn alle Formulare zentral gespeichert sind (automatische Aktualisierungen), müssen Benutzer nur eine zentrale Stelle nach neuen Formularen durchsuchen. Wenn ein neues Formular zur Verfügung gestellt wird, können alle Clients, die an dieser Stelle suchen, sofort darauf zugreifen. Der Nachteil ist, dass viele Formulare angezeigt werden, die für den Benutzer nicht relevant sind.
- **Manuelle Aktualisierung:** Wenn Formulare lokal gespeichert sind (manuelle Aktualisierungen), müssen Sie die Formulare an die Benutzer verteilen, die sie ausfüllen müssen. Dadurch wird das Netzwerk weniger belastet, weil jeder Client eine eigene Kopie des Formulars besitzt. Der Vorteil von lokalen Kopien besteht darin, dass Sie die Formulare, die den Benutzern angezeigt werden, auf die für sie relevanten Formulare beschränken können. Formulare können beim Clientsetup oder mit dem Tool "Geplante Tasks" auf Clients kopiert werden.

Sie müssen außerdem angeben, wann Formulare auf dem Client angezeigt werden:

- **Beim Start:** Die Formularanzeige des Clients sucht bei jedem Start nach neuen oder geänderten Formularen. Die Formularanzeige wird nach dem Laden des Betriebssystems gestartet. Wenn der Inventarscanner das nächste Mal ausgeführt wird, sendet er ausgefüllte Formulare an die Core-Datenbank.
- **Wenn der Inventarscanner ausgeführt wird:** Der Inventarscanner startet die Formularanzeige, die nach neuen oder geänderten Formularen sucht. Sobald Benutzer das Formular komplett ausgefüllt und die Formularanzeige geschlossen haben, wird der Scan beendet, und die Daten werden in die Core-Datenbank eingegeben.
- **Nur im LANDesk-Programmordner:** Die Formularanzeige kann manuell über die LANDesk Management Suite-Programmgruppe gestartet werden. Wenn der Inventarscanner das nächste Mal ausgeführt wird, sendet er ausgefüllte Formulare an die Core-Datenbank.

Sie können auch die Funktion "Geplante Tasks" verwenden, um die Formularanzeige zu einer vorgegebenen Zeit auf Clients starten. Verwenden Sie in diesem Szenario "Geplante Tasks", um die Formulare zuerst an Clients zu verteilen. Räumen Sie genügend Zeit für die Verteilung der Formulare ein, bevor Sie die skriptfähige Aufgabe von "Geplante Tasks" verwenden, um die Formularanzeige auszuführen.

Ausfüllen von Formularen auf dem Client

Wenn die Formularanzeige auf dem Client gestartet wird, wird eine Liste der Formulare und der Status der einzelnen Formulare angezeigt.

- **Neu:** Gibt an, dass das Formular von diesem Benutzer noch nie ausgefüllt wurde.
- **Abgeschlossen:** Gibt an, dass der Benutzer dieses Formular geöffnet und zumindest die erforderlichen Felder ausgefüllt hat.
- **Wiederholen:** Gibt an, dass der Benutzer dieses Formular bereits ausgefüllt hat, das Formular sich seither jedoch geändert hat. Der Benutzer muss sich das Formular erneut ansehen und gegebenenfalls Änderungen eingeben. Sobald dies geschehen ist, ändert sich der Status zu "Abgeschlossen".

Sobald Benutzer ein auszufüllendes Formular auswählen und auf "Öffnen" klicken, wird ein einfacher Formularassistent angezeigt. Er enthält eine Fragenliste und Felder für Antworten. Wenn die Fragen auf mehrere Seiten verteilt sind, gibt es die Schaltflächen "Zurück" bzw. "Weiter". Wenn sich der Cursor in einem Feld befindet, während die Benutzer auf "Hilfe" klicken (oder F1 drücken), wird eine Hilfemeldung angezeigt, die vom Feld "Beschreibung" im Form Designer generiert wurde.

Die Benutzer müssen alle Fragen in erforderlichen Feldern beantworten, bevor sie zur nächsten Seite wechseln oder ein Formular schließen. Fragen in erforderlichen Feldern sind durch einen roten Punkt gekennzeichnet.

Auf der letzten Seite des Formularassistenten gibt es eine Schaltfläche "Beenden", auf die Benutzer klicken müssen, wenn sie fertig sind. Wenn die Benutzer auf diese Schaltfläche klicken, wird wieder das Dialogfeld "Formularauswahl" mit einer aktualisierten Statusmeldung neben dem Formularnamen angezeigt.

Übersicht über Berichte

Management Suite enthält ein leistungsfähiges Berichterstellungstool, mit dem Sie Berichte auf den Clients im Netzwerk auswählen und ausführen können.

Sie können aus einer Vielzahl von vordefinierten LANDesk Management Suite(LDMS)-Dienstberichten und -Inventaranlagenberichten auswählen oder eigene, benutzerdefinierte Inventarberichte erstellen. Außerdem können Sie Berichte in benutzerdefinierten Gruppen zusammenfassen.

In diesem Abschnitt erfahren Sie mehr über:

- Berichtsgruppen und vordefinierte Berichtslisten
- Erstellen von benutzerdefinierten Inventarberichten
- Ausführen von Berichten
- Verwenden der Berichtsansicht
- Importieren und Exportieren von Berichten

Berichtsgruppen und vordefinierte Berichtslisten

Berichte werden im Fenster "Berichte" (**Extras | Berichte**) in Gruppen organisiert. Administratoren können den Inhalt aller Berichtsgruppen einsehen. Benutzer mit Zugriffsrecht auf Berichte können außerdem auf Geräten in ihrem Bereich Berichte anzeigen und ausführen.

Sie können neue Berichte erstellen, indem Sie mit der rechten Maustaste auf "Berichte" und anschließend auf "Eigene Berichte" oder "Alle benutzerdefinierten Berichte" klicken und **Neuer Bericht** wählen. Wenn Sie einen neuen Bericht erstellen, wird er automatisch der Gruppe "Alle benutzerdefinierten Berichte" hinzugefügt.

Der linke Bereich des Fensters "Berichte" zeigt eine hierarchische Ansicht der folgenden Berichtsgruppen:

Eigene Berichte

Zeigt die Berichte (und Berichtsgruppen), die ein Benutzer zu seiner Gruppe "Eigene Berichte" hinzugefügt hat. Berichte werden auf den Bereich des aktuell angemeldeten Benutzers ausgeführt.

Ein Administrator kann Berichte zu Berichtsgruppen eines Benutzers hinzufügen oder sie daraus entfernen (siehe "Benutzerberichte" weiter unten).

Alle LDMS-Berichte

Zeigt alle vordefinierten Management Suite-Berichte. Administratoren und Benutzer mit Zugriffsrecht auf Berichte können alle LDMS-Berichte anzeigen. LDMS-Berichte enthalten Statusinformationen zu verschiedenen Management Suite-Dienstaufträgen, -Aktionen oder -Ereignissen, die auf Clients im Netzwerk ausgeführt werden. Dazu gehören folgende Berichte:

APM-Status

- **APM-Status nach Rechner:** Zeigt nach ausgewählten Geräten die auf den Geräten ausgeführten Richtlinien zusammen mit dem damit verknüpften Benutzer, auf den die Richtlinie ausgeführt wurde, den letzten Ausführungszeitpunkt und den Status der Richtlinie.
- **APM-Status nach Richtlinie:** Zeigt nach ausgewählten Richtlinien die Geräte, auf denen die Richtlinien ausgeführt wurden zusammen mit dem damit verknüpften Benutzer, auf den die Richtlinie ausgeführt wurde, den letzten Ausführungszeitpunkt und den Status der Richtlinie.
- **APM-Status nach Benutzer:** Zeigt nach ausgewähltem Benutzer die Richtlinien, die auf den Benutzer ausgeführt wurden zusammen mit den betroffenen Geräten, den letzten Aktualisierungszeitpunkt und den Status der Richtlinie.
- **APM-Statusbericht – Alle Richtlinien:** Zeigt nach Richtlinie und Gerät die Benutzer, auf die die Richtlinie ausgeführt wurde, den letzten Ausführungszeitpunkt und den Status der Richtlinie.

Application Healing

- **Pro Client reparierte Anwendungen:** Zeigt nach ausgewähltem Datum die Geräte, auf denen Application Healing-Tasks ausgeführt wurden zusammen mit den erfolgreichen, fehlgeschlagenen und abgebrochenen Reparaturprozessen.
- **Listenbericht "Beschädigte Anwendungen":** Zeigt für alle Geräte die beschädigten Anwendungen und wie häufig sie als beschädigt gemeldet wurden.
- **Client-Ereignisprotokoll:** Zeigt nach Gerät jedes Ereignis, das auf einem Gerät stattgefunden hat, zusammen mit etwaigen Systemfehlern, AutoInstall-Fehlern oder Ereigniscodemeldungen.
- **Pro Anwendung reparierte Computer:** Zeigt nach Produkt die Geräte, die mit dem Produkt repariert wurden, die Anzahl der erfolgreichen, fehlgeschlagenen und abgebrochenen Reparaturversuche für die Geräte und den Zeitpunkt der zuletzt durchgeführten Reparatur.

Multicast-Clientstatus

Repräsentativer Status des Multicast-Subnetzes

OS-Verteilungserfolgsrate

Skriptfähiger Aufgabenstatus

Anstelle von vordefinierten Berichten enthalten die obigen Berichtsgruppen Protokolldateien für geplante Tasks (entsprechend der Gruppenkategorie), die auf Ihrem Management Suite-System ausgeführt wurden. Die Nummer des Protokolls entspricht der Auftragsnummer der geplanten Task, auf die sich das Protokoll bezieht. Sie können mit der rechten Maustaste auf ein Protokoll klicken und "Ausführen" auswählen, um basierend auf den Daten der Protokolldatei einen Bericht zu erstellen.

Hinweis: Alle Protokolldateien werden im Verzeichnis \LANDesk\ManagementSuite\log gespeichert.

Alle Anlagenberichte

Zeigt alle vordefinierten Inventaranlagenberichte. Administratoren und Benutzer mit Zugriffsrecht auf Berichte können alle Inventarberichte anzeigen. Inventarberichte liefern Inventarinformationen über Clients im Netzwerk.

Hinweis: Inventaranlagenberichte sind Crystal Reports*-Vorlagen von Inventarattributen. Ein Bericht besteht aus einer Abfragedatei (.QRY), einer Datendefinitionsdatei (.TTX) und einer Berichtsvorlagendatei (.RPT). Mit Crystal Reports 9 von Crystal Decisions können Sie weitere Berichte zur Anzeige im Dialogfeld "Berichte" erstellen.

Es gibt mehr als 50 verschiedene vordefinierte Inventaranlagenberichten.

- **Programme nach Computern hinzufügen/entfernen:** Zeigt für ein ausgewähltes Gerät alle Programme, die im Fenster "Software" in der Systemsteuerung enthalten sind.
- **Anti-Virusprogrammübersicht:** Zeigt nach ausgewählten Programmen die auf den Geräten im Bereich des Benutzers installierte Anti-Virussoftware.
- **BIOS-Übersicht:** Zeigt nach BIOS-Hersteller für alle Geräte im Bereich des Benutzers den BIOS-Urheberrechtsvermerk und das Datum.
- **Computerinstallationen nach Datei:** Zeigt nach ausgewählter Datei alle Instanzen der Datei auf allen Geräten im Bereich des Benutzers.
- **Computerinstallationen nach Produkt:** Zeigt nach Produkt für alle Geräte im Bereich des Benutzers jede Instanz jedes Programms.
- **Computerinstallationen nach Anbieter:** Zeigt die Anzahl der Kopien eines Programms nach Entwickler für alle Geräte im Bereich des Benutzers.
- **Computer-Betriebssysteme:** Listet die Computer auf, die von Ihnen angegebene Betriebssysteme verwenden.
- **Software-Übersicht:** Zeigt alle Programme für das ausgewählte Gerät.
- **Computer nach LDMS-Clientversion:** Zeigt alle Geräte im Bereich des Benutzers nach Scannerversion.
- **Computer für einen bestimmten Benutzer:** Zeigt für den primären Eigentümer die Geräte im Bereich des Benutzers zusammen mit der Domäne oder dem Arbeitsgruppenort der Geräte.
- **Computer in Domäne oder Arbeitsgruppe:** Zeigt für die ausgewählten Domänen und/oder Arbeitsgruppen die Geräte im Bereich des Benutzers, die Mitglied einer bestimmten Domäne oder Arbeitsgruppe sind.
- **Computer in Subnetz:** Zeigt nach Subnetz alle Geräte im Bereich des Benutzers, die Mitglied des entsprechenden Subnetzes sind.
- **Computer, die einen bestimmten Dienst ausführen:** Zeigt für ausgewählten Dienste alle Geräte im Bereich des Benutzers, die in ihrem Betriebssystem über einen bestimmten Dienst verfügen.
- **Computer, die auf Windows 2000 aufgerüstet werden können:** Zeigt alle Geräte im Bereich des Benutzers, die die Festplatten-, Speicher- und Prozessor-Mindestanforderungen für Windows 2000 erfüllen.
- **Computer, die nicht auf Windows XP aufgerüstet werden können:** Zeigt alle Geräte im Bereich des Benutzers, die die Festplatten-, Speicher- und Prozessor-Mindestanforderungen für Windows XP erfüllen.
- **Computer, die nicht auf Windows 2000 aufgerüstet werden können:** Zeigt alle Geräte im Bereich des Benutzers, die die Festplatten-, Speicher- und Prozessor-Mindestanforderungen für Windows 2000 nicht erfüllen.
- **Computer, die nicht auf Windows XP aufgerüstet werden können:** Zeigt alle Geräte im Bereich des Benutzers, die die Festplatten-, Speicher- und Prozessor-Mindestanforderungen für Windows XP nicht erfüllen.
- **Computer mit bestimmter Festplattengröße:** Listet Computer, deren Festplatte die von Ihnen angegebene Größe aufweist.
- **Computer mit doppelten Gerätekennungen:** Zeigt alle doppelten Gerätenamen im Bereich des Benutzers.
- **Tage seit letztem Hardware-Scannen:** Zeigt nach ausgewähltem Zeitraum, wann der letzte Hardware-Scan auf allen Geräten im Bereich des Benutzers ausgeführt wurde.
- **Tage seit letztem Software-Scannen:** Zeigt nach ausgewähltem Zeitraum, wann der letzte Software-Scan auf allen Geräten im Bereich des Benutzers ausgeführt wurde.
- **Plattenplatzübersicht:** Zeigt den gesamten Festplattenspeicher und die verfügbare Speicherkapazität für alle Geräte im Bereich des Benutzers.

- **Domänenbenutzer:** Zeigt alle Benutzer in einer bestimmten Domäne.
- **Hardware-Inventar:** Zeigt verschiedene Hardware-Spezifikationen für alle Geräte im Bereich des Benutzers.
- **Hotfix installiert:** Zeigt nach Hotfix alle Hotfixes, die auf den Geräten im Bereich des Benutzers installiert sind.
- **IP-Adressenübersicht:** Zeigt nach Subnetz die IP- und NIC-Adresse für alle Geräte im Bereich des Benutzers.
- **Macintosh-Plattenplatz:** Zeigt den gesamten Festplattenspeicher und die verfügbare Speicherkapazität für alle Macintosh-Geräte im Bereich des Benutzers.
- **Macintosh-Hardware-Inventarübersicht:** Zeigt verschiedene Hardware-Spezifikationen für alle Macintosh-Geräte im Bereich des Benutzers.
- **Hersteller:** Zeigt nach Hersteller alle Geräte im Bereich des Benutzers zusammen mit ihrer Computermodellbeschreibung und ihrem Betriebssystem.
- **Speicher-Upgrade:** Zeigt den insgesamt verfügbaren Speicher sowie die Anzahl der verwendeten und verfügbaren RAM-Steckplätze für alle Geräte im Bereich des Benutzers.
- **Betriebssystem nach Service Pack:** Zeigt alle Geräte im Bereich des Benutzers nach Service Pack.
- **Betriebssystemübersicht:** Zeigt alle Geräte im Bereich des Benutzers nach Betriebssystem.
- **Peripheriegeräte-Übersicht:** Zeigt nach Gerät Informationen über Modem, Drucker, Soundkarte, Tastatur und Netzwerkadapter, die an ein Gerät angeschlossen sind, für alle Geräte im Bereich des Benutzers.
- **Physikalischer Speicher:** Zeigt die Größe des Speichers nach Speicherbereich für alle Geräte im Bereich des Benutzers.
- **Prozessorverteilung:** Zeigt nach Prozessortyp alle Geräte im Bereich des Benutzers einschließlich Prozessorgeschwindigkeit.
- **Prozessorgeschwindigkeit:** Zeigt für alle Geräte im Bereich des Benutzers die Prozessorgeschwindigkeit nach Prozessorgeschwindigkeitsbereich.
- **Prozessorübersicht:** Zeigt nach Gerät verschiedene Informationen über die CPU für alle Geräte im Bereich des Benutzers.
- **Prozessortyp:** Zeigt den Prozessortyp nach Prozessorklasse (Pentium II, Pentium 4 usw.) für alle Geräte im Bereich des Benutzers.
- **Prozessortyp und -geschwindigkeit:** Zeigt die Anzahl der Prozessortypen nach Geschwindigkeit für alle Geräte im Bereich des Benutzers.
- **Subnetze nach Subnetzmaske:** Zeigt nach Subnetzmaske alle Subnetze einer Maske.
- **Systembestandskennzeichen:** Zeigt den aktuellen oder letzten Anmeldenamen, die Seriennummer und das Bestandskennzeichen für alle Geräte im Bereich des Benutzers.
- **Systemseriennummer:** Zeigt den aktuellen oder letzten Anmeldenamen, die Seriennummer und die Domäne oder Arbeitsgruppe für alle Geräte im Bereich des Benutzers.
- **Benutzer in ausgewählter Domäne:** Zeigt nach Domäne alle Benutzer in einer bestimmten Domäne.
- **Videoadaptertyp-Übersicht:** Zeigt nach Videoadapter alle Geräte im Bereich des Benutzers, die über einen bestimmten Videoadapter verfügen, sowie den Gesamtspeicher des Videoadapters.
- **Videospeicher-Übersicht:** Zeigt nach Videogesamtspeicher alle Geräte im Bereich des Benutzers, die über eine bestimmte Videospeicherkapazität verfügen.

- **Videoübersicht:** Zeigt nach Gerät für alle Geräte im Bereich des Benutzers verschiedene Informationen über den Videoadapter.

Alle Softwarelizenzierungsberichte

Zeigt alle vordefinierten Softwarelizenzüberwachungsberichte einschließlich:

- **Anwendungsverwendung pro Computer:** Zeigt nach ausgewähltem Gerät die Produkte, die auf dem Gerät ausgeführt werden nach Name, Anzahl der Ausführungen und Dauer der Verwendung.
- **In den letzten n Tagen verwendete Anwendungen:** Zeigt nach der ausgewählten Anzahl der Tage für alle Geräte die verwendeten Produkte sowie Datum und Uhrzeit ihrer letzten Verwendung.
- **Nicht öfter als n Mal verwendete Anwendungen:** Zeigt nach ausgewähltem Produkt und Zeitspanne für die Verwendung des Produkts, wie oft das ausgewählte Produkt auf allen Geräten verwendet wurde.
- **Verweigerungsbericht:** Zeigt nach ausgewähltem Produkt alle Geräte, die melden, dass versucht wurde, das ausgewählte Produkt auszuführen, zusammen mit dem entsprechenden Benutzer und der Anzahl der Verweigerungen.
- **Gruppenerfüllung:** Zeigt nach ausgewählter Produktgruppe die Produkte in der Gruppe zusammen mit der Anzahl der Lizenzen und Installationen sowie die Anzahl der Produkte, die nicht den Bestimmungen entsprechend verwendet werden, und der Lizenzen, die nicht verwendet werden.
- **Lizenzproduktverwendung pro Produkt:** Zeigt nach ausgewähltem Produkt alle Geräte, die über das ausgewählte Produkt verfügen, den letzten Zeitpunkt, zu dem das Produkt verwendet wurde, den letzten Benutzer des Produkts, wie häufig das Produkt ausgeführt wurde, wie lange das Produkt ausgeführt wurde und die Anzahl der Tage, seitdem das Produkt zum letzten Mal verwendet wurde.
- **Lizenziertes Produkt, das Herabstufungsrechte verwendet:** Zeigt für alle Produkte, die eine Herabstufung verwenden, die Anzahl der geliehenen Lizenzen sowie, von welchem Produkt die Lizenzen geliehen sind.
- **Nicht überall bereitgestellte Lizenzen:** Zeigt für alle Produktgruppen die Anzahl der von jeder Gruppe nicht bereitgestellten Lizenzen.
- **Nicht pro Gruppe verteilte Lizenzen:** Zeigt nach ausgewählter Produktgruppe die für jedes Produkt in der Gruppe nicht bereitgestellten Lizenzen.
- **Gesamt-Erfüllung:** Zeigt für alle Produktgruppen, ob die Gruppe die Bestimmungen einhält, die Anzahl der Geräte, die die Bestimmungen nicht einhalten, und die Anzahl der nicht bereitgestellten Lizenzen.

Hinweis: Softwarelizenzüberwachungsberichte werden durch Benutzerbereiche nicht beschränkt.

Fernsteuerungsagent

Zeigt alle Fernsteuerungsberichte:

- **Fernsteuerungsverlauf nach Client:** Zeigt den Fernsteuerungsverlauf für alle Clients innerhalb eines bestimmten Datumsbereichs.

- **Fernsteuerungsverlauf nach Konsole:** Zeigt den Fernsteuerungsverlauf für alle Konsolen innerhalb eines bestimmten Datumsbereichs.
- **Fernsteuerungsverlauf nach verwaltete Computer:** Zeigt den Fernsteuerungsverlauf für einen bestimmten Client.
- **Fernsteuerungsübersicht:** Zeigt eine Zusammenfassung des Fernsteuerungsverlaufs innerhalb eines bestimmten Datumsbereichs.

Alle Erkennung nicht verwalteter Geräte Berichte

Zeigt alle Berichte zur nicht verwalteten Geräteerkennung:

- **Nicht verwaltete Geräte - Computer:** Zeigt alle Computer in der Struktur "Computer" von UDD.
- **Nicht verwaltete Geräte - Infrastruktur:** Zeigt alle Infrastruktur-Netzwerkgeräte in der Struktur "Infrastruktur" von UDD, beispielsweise Router.
- **Nicht verwaltete Geräte - Sonstige:** Zeigt alle Geräte in der Struktur "Sonstige" von UDD. Es handelt sich hierbei um Geräte, mit mehr als einer IP-Adresse, die nicht auf eine Erkennung reagieren. Beispielsweise Macintosh- oder UNIX-Computer.
- **Nicht verwaltete Geräte - Drucker:** Zeigt alle Drucker in der Struktur "Drucker" von UDD.
- **Nicht verwaltete Systeme:** Zeigt alle Geräte im Netzwerk, die keinem Core Server zugeordnet sind.
- **Nicht verwaltete Systeme mit LANDesk Client Agent (CBA):** Zeigt alle Computer in der Struktur "Computer" von UDD, auf denen der Management Suite CBA-Agent installiert ist.
- **Nicht verwaltete Systeme ohne LANDesk Client Agent (CBA):** Zeigt alle Computer in der Struktur "Computer" von UDD, auf denen der Management Suite CBA-Agent nicht installiert ist.

Alle benutzerdefinierten Berichte

Zeigt alle benutzerdefinierten Berichte, die Sie erstellt oder importiert haben. Weitere Informationen finden Sie unter "Erstellen von benutzerdefinierten Inventarberichten" im nächsten Abschnitt.

Benutzerberichte

Zeigt alle Berichte für alle Management Suite-Benutzer; sie werden nach Benutzern in Untergruppen unterteilt. Benutzeruntergruppen werden mit ihren Anmelde-IDs benannt (d.h. Computername\Benutzerkonto oder Domäne\Benutzerkonto). Jede Benutzergruppe enthält die Berichte, die in der Gruppe "Eigene Berichte" des jeweiligen Benutzers angezeigt werden.

Wie die Gruppen "Benutzergeräte" und "Benutzerabfragen" wird auch die Gruppe "Benutzerberichte" NUR dem Management Suite-Administrator (einem Benutzer mit LANDesk-Administratorrechten) angezeigt. Administratoren können auf die Berichtsgruppe eines Benutzers zugreifen, um Berichte auf den Bereich des Benutzers auszuführen, als wären sie dieser Benutzer. So kann ein Administrator genau sehen, was ein Benutzer sieht, wenn er einen Bericht ausführt.

Erstellen von benutzerdefinierten Inventarberichten

Sie können eigene, benutzerdefinierte Inventaranlagenberichte basierend auf von Ihnen festgelegten Spaltenkonfigurationen erstellen, mit denen die in der Netzwerkansicht angezeigten Inventardaten festgelegt werden. Diese Berichte werden als generische .CSV-Dateien gespeichert.

Wenn Crystal Reports (Version 9) auf Ihrem Computer installiert ist, können Sie komplexere Inventarberichte basierend auf Core-Datenbankabfragen erstellen. Falls Crystal Reports nicht installiert ist, ist diese Funktion deaktiviert.

Erstellen von .CSV-Berichten

So erstellen Sie einen .CSV-Inventarbericht

1. Klicken Sie im Fenster "Berichte" auf **Berichte** und anschließend in der Symbolleiste auf die Schaltfläche **Neuer CSV-Bericht**.
2. Geben Sie im Dialogfeld "Neuer CSV-Bericht" einen Namen für den Bericht ein.
3. Geben Sie an, ob der Bericht alle oder nur bestimmte Geräte umfassen soll.
4. Legen Sie fest, ob die aktuelle oder eine andere Spaltenkonfiguration in der Netzwerkansicht verwendet werden soll.
5. Klicken Sie auf **OK**, um die .CSV-Datei mit dem von Ihnen angegebenen Namen und Verzeichnis zu speichern.

Hinweis: Sie können auch einen .CSV-Inventarbericht zur Verwendung in anderen Berichterstellungstools exportieren.

Informationen zum Dialogfeld "Neuer CSV-Bericht"

In diesem Dialogfeld erstellen Sie einen .CSV-Inventarbericht.

- **Dateiname:** Geben Sie einen eindeutigen Dateinamen am Ende des bestehenden Pfads ein. Wenn es den Verzeichnispfad noch nicht gibt, werden Sie aufgefordert, ihn zu erstellen.
- **Bericht für Geräte:** Legt fest, ob der Bericht für alle Geräte oder nur für die derzeit in der Netzwerkansicht ausgewählten Geräte ausgeführt wird.
- **Spaltenkonfiguration:** Legt basierend auf der Spaltenkonfiguration fest, welche Inventardaten im Bericht erfasst werden sollen. Sie können die aktuelle Spaltenkonfiguration verwenden oder eine andere Spaltenkonfiguration auswählen.
- **OK:** Speichert den Bericht und schließt das Dialogfeld.
- **Abbrechen:** Speichert das Dialogfeld, ohne den Bericht zu speichern.

Erstellen von Crystal Reports

So erstellen Sie einen Crystal Reports-Inventarbericht

1. Klicken Sie im Fenster "Berichte" auf **Berichte** und anschließend in der Symbolleiste auf die Schaltfläche **Neuer Crystal Report**.
2. Geben Sie im Dialogfeld "Neuer Crystal Report" einen eindeutigen Namen für den Bericht ein.
3. Wählen Sie die Core-Datenbankabfrage aus, auf der der Bericht basieren soll. Sie können eine neue Abfrage erstellen oder eine bestehende Abfrage verwenden. Wenn Sie keine Abfrage auswählen, liefert der Bericht Ergebnisse für alle Geräte im Bereich des Benutzers.

   Beim Erstellen eines Crystal Reports müssen Sie mindestens eine Spalte für den Bericht festlegen.

4. Klicken Sie auf **Crystal Reports starten**, um den Crystal Reports-Assistenten zu starten.
5. Führen Sie die Schritte im Dialogfeld "Neuer Crystal Report" aus. Wenn Sie ausführlichere Informationen benötigen, können Sie im Crystal Reports-Assistenten auf **Hilfe** klicken.

Informationen zum Dialogfeld "Neuer Crystal Report"

In diesem Dialogfeld erstellen Sie einen Crystal Report-Inventarbericht.

- **Name:** Geben Sie einen eindeutigen Namen für den Bericht ein.
- **Abfragename:** Legt die Daten fest, die für die ausgewählten Geräte erfasst werden. Sie können entweder eine neue Abfrage erstellen oder eine bestehende Abfrage bearbeiten oder auswählen.
- **Crystal Reports starten:** Startet den Crystal Reports-Assistenten. Führen Sie die Schritte im Dialogfeld aus, um den Bericht zu erstellen.

Ausführen von Berichten

Sie können jeden Bericht aus dem Fenster "Berichte" ausführen. In der Netzwerkansicht können Sie Inventarberichte aber auch direkt von einem Gerät ausführen.

Im Fenster "Berichte" klicken Sie mit der rechten Maustaste auf den gewünschten Bericht, anschließend klicken Sie auf **Ausführen** (Sie können auch die Schaltfläche **Ausführen** in der Symbolleiste verwenden). Die Berichtsdaten werden in der Berichtsansicht angezeigt.

Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf das Gerät, klicken Sie anschließend auf **Anlagenbericht ausführen**, und doppelklicken Sie im Dialogfeld "Bericht" auf den Bericht, der ausgeführt werden soll. Die Berichtsdaten werden in der Berichtsansicht angezeigt.

Verwenden der Berichtsansicht

Die Berichtsansicht enthält folgende Symbolleistenfunktionen:

- **Durchsuchen:** Damit können Sie den Bericht Seite für Seite oder nach Berichtskomponente (Client, Software, Benutzer usw.) lesen.
- **Drucken:** Öffnet ein Standarddruckdialogfeld.
- **Exportieren:** Öffnet ein Exportdialogfeld, in dem Sie die Berichtsdaten in eine Crystal Reports-Datei, eine PDF-Datei, eine Excel-Tabelle, ein Word-Dokument oder eine RTF-Datei speichern können.
- **Suche:** Ermöglicht die Suche nach einer bestimmten Textzeichenfolge in den Berichtsdaten.

Importieren und Exportieren von Berichten

Das Management Suite-Berichterstellungstool unterstützt das Importieren und Exportieren von Crystal Reports. Crystal Reports werden als XML-Berichtsdateien gespeichert. Über das Importieren und Exportieren können Sie Berichte aus einer Core-Datenbank in eine andere übertragen.

Ein Bericht kann in die Gruppen "Eigene Berichte", "Alle benutzerdefinierten Berichte" und "Benutzerberichte" importiert werden.

So importieren Sie einen Crystal Report

1. Klicken Sie mit der rechten Maustaste auf die Berichtsgruppe, in welche der Bericht importiert werden soll.
2. Wählen Sie **Importieren** aus dem Kontextmenü (oder aus der Symbolleiste).
3. Navigieren Sie zur Berichtsdatei (.XML), die Sie importieren möchten, und wählen Sie sie aus.
4. Klicken Sie auf **Öffnen**, um den Bericht in der Netzwerkansicht zu der ausgewählten Gruppe hinzuzufügen.

Sie können sowohl einzelne Berichte als auch ganze Berichtsgruppen und deren Inhalt exportieren.

So exportieren Sie einen Crystal Report

1. Klicken Sie mit der rechten Maustaste auf den Crystal Report (oder die Berichtsgruppe), den (die) Sie exportieren möchten.
2. Wählen Sie **Exportieren** aus dem Kontextmenü (oder aus der Symbolleiste).
3. Navigieren Sie zu dem Speicherort, an dem der Bericht gespeichert werden soll.
4. Geben Sie einen Namen für den Bericht ein.
5. Klicken Sie auf **Speichern**, um den Bericht zu exportieren.

Kapitel 5: Fernverwaltung

Mit der Fernsteuerungsfunktion von LANDesk Management Suite können Sie Clientprobleme von einem Ort aus leicht lösen. In diesem Kapitel erfahren Sie mehr über:

- Fernsteuerung von Clients
- Starten einer Fernsteuerungssitzung
- Anzeigen von Sitzungsmeldungen
- Fernausführung von Programmen
- Chat mit Fernclients
- Übertragen von Dateien auf Fernclients
- Herunterfahren und Neustarten von Fernclients
- Konfiguration der Sitzungsoptionen
- Ändern der Client-Fernsteuerungssicherheit
- Konfigurieren der Mac OS X-Fernsteuerungsoptionen
- Verwenden der Fernsteuerungsprotokollierung
- Fehlerkorrektur bei Fernsteuerungssitzungen

Fernsteuerung von Clients

Mit der Fernsteuerung erhalten Sie von der Konsole Fernzugriff auf einen Client. Sie können nur Clients fernsteuern, auf denen der Fernsteuerungsagent installiert ist. Während einer Fernsteuerungssitzung verfügt der Client über zwei Benutzer - Sie und den Endbenutzer. Sie können alles auf dem Fernclient tun, was der Benutzer am Client auch tun kann. Alle Ihre Aktionen erfolgen auf dem Client in Echtzeit.

Management Suite ermöglicht Ihnen, diese Clientarten fernzusteuern.

- Windows NT-/2000-/2003-/XP-Clients
- Windows 95/98-Clients
- NetWare-Server
- Mac OS 8, 9.2.2, 10.2.x und 10.3.x Clients

Videounterstützung
Die Fernsteuerung unterstützt keine DOS-Grafiken. Sie unterstützt auch keine Vollbild-DOS-Fenster.

Für die Fernsteuerung muss der Client folgende Eigenschaften aufweisen:

- **Die LANDesk-Agenten müssen geladen sein** - Diese Agenten werden installiert und eingerichtet von:
  - Erstellen eines Client-Konfigurationstask in der Konsole und Push-Verteilung auf den Client.
  - Zuordnung eines Laufwerks vom Client an den Core Server und Ausführung der entsprechenden Clientkonfiguration.
- **Fernsteuerung zulassen**—Sofern es die Fernsteuerungskonfiguration des Client zulässt, können Benutzer mithilfe der Anwendung "Fernsteuerungseinstellungen" Fernsteuerungszugriffs- und kontrollparameter festlegen. Benutzer können diese Anwendung auf dem Client öffnen, indem sie auf **Start | Programme | LANDesk Management | Fernsteuerungseinstellungen** klicken oder EDTININT.EXE direkt ausführen.

LANDesk Management Suite 8 unterstützt keine NetWare-Sicherheit für die Fernsteuerung mehr.

Macintosh-Unterstützung

Die folgende Tabelle beschreibt die Macintosh-Unterstützung für die Remote Control Viewer-Funktionen:

Funktion	Mac OS 8 und 9.2.2	Mac OS X 10.2.x und 10.3.x
Fernsteuerung	Ja	Ja
Dateiübertragung	Ja	Ja
Fernausführung	Ja	Ja
Chat	Nein	Ja
Fernneustart	Nein	Ja

Mac OS 8- und 9.2.2-Clients unterstützen keinen Chat und keinen Fernneustart.
Die Chat- und Neustartschaltflächen des Remote Control Viewer-Fensters funktionieren nicht, wenn Mac OS 8- und 9.2.2-Clients gesteuert werden.

Starten einer Fernsteuerungssitzung

Wenn der Fernsteuerungsagent geladen ist, teilt Ihnen das Fenster "Sitzungsmeldungen" mit, dass der Agent gefunden wurde und welches Protokoll verwendet wird. Auf dem ausgewählten Client erscheint auch ein Lupensymbol.

So sehen Sie, ob der Fernsteuerungsagent geladen ist

1. Klicken Sie in der Netzwerkansicht der Konsole auf den **Client**, den Sie überprüfen möchten.
2. Klicken Sie auf **Anzeigen | Sitzungsmeldungen**.

Weitere Informationen zum Fenster "Sitzungsmeldungen" finden Sie unter "Anzeigen von Sitzungsmeldungen" weiter unten in diesem Kapitel.

So starten Sie die Fernsteuerung

1. Wählen Sie in der Netzwerkansicht der Konsole den **Client**, den Sie steuern möchten. Klicken Sie auf **Gerät | Fernsteuerung**, um das Fenster "Remote Control Viewer" zu öffnen.
2. Geben Sie im Bearbeitungsfeld oben im Viewer-Fenster den Namen oder die IP-Adresse eines Fernclients ein.
3. Klicken Sie auf **Extras | Fernsteuerung**, um auf den Fernclient zuzugreifen.

Wenn Sie einen Fernclient steuern, wird dessen Bildschirm im Viewer-Fenster angezeigt. Da das Viewer-Fenster in der Regel kleiner ist als der Bildschirm des Fernclients, müssen Sie entweder "Autoscroll" zum Scrollen aktivieren oder das Symbol "Fernbildschirm verschieben" verwenden, um die verschiedenen Bereiche des Fernbildschirms anzuzeigen.

Wenn Sie die Anzeigegeschwindigkeit erhöhen oder die Einstellungen des Viewer-Fensters ändern möchten, nutzen Sie die Elemente unter dem Menü "Optionen". Für einen Fernchat, Ferndateitransfer oder Fernneustart des Clients nutzen Sie die Elemente unter dem Menü "Extras".

So zeigen Sie die verschiedenen Bereiche eines Fernclientbildschirms an

Damit diese Option funktioniert, müssen Sie derzeit einen Client fernsteuern.

- Klicken Sie auf **Optionen | Autoscroll**. Wenn aktiviert, ermöglicht Ihnen Autoscroll, den Cursor entlang des gelb-schwarzen Rands des Viewer-Fensters zu platzieren und nach oben, unten, links oder rechts zu scrollen. Je dichter Ihr Cursor an den Rand gelangt, umso schneller ist der Scrollvorgang.

ODER

1. Klicken Sie auf der rechten Seite des Bearbeitungsfeldes (wo Sie den Namen des Fernclients eingegeben haben) auf das Symbol **Fernbildschirm verschieben**.
2. Der Cursor verwandelt sich in eine Hand, sodass Sie mit Klicken, Ziehen und Loslassen zu den verschiedenen Bereichen des Fernbildschirms wechseln können.

So beenden Sie eine Fernsteuerungssitzung

- Klicken Sie erneut auf **Extras | Fernsteuerung**. Obwohl diese Aktion die aktive Sitzung beendet, sind Sie so lange noch mit dem Fernclient verbunden, bis Sie einen neuen Clientnamen oder eine IP-Adresse eingeben bzw. das Viewer-Fenster schließen.

Anzeigen von Sitzungsmeldungen

Sie können mit dem Abschnitt "Sitzungsmeldungen" des Ansichtsfensters einen Verlauf der an die Statusleiste gesendeten Statusmeldungen einblenden (wie z. B. Fernsteuerungsagent-Paketaustausche). Neben anderen in dieser Historie enthaltenen Informationen können Sie folgende Aktionen durchführen:

- Diagnostizierung von Problemen bei der Sitzung
- Überprüfung, ob der Fernsteuerungsagent geladen ist
- Überprüfung des Status des Fernsteuerungsagenten

So zeigen Sie Sitzungsmeldungen von der Konsole aus an

- Klicken Sie im Ansichtsfenster auf **Ansicht | Sitzungsmeldungen.**

Speichern von Sitzungsmeldungen

Während Sie eine Fernsteuerungssitzung ausführen, haben Sie die Möglichkeit, die Sitzungsmeldungen zu speichern. Die Meldungen können dann hilfreich sein, wenn Sie Fehler beheben möchten, die sich auf den Einsatz einer Fernsteuerung auf einem bestimmten Client beziehen.

So speichern Sie Sitzungsmeldungen

1. Klicken Sie im Viewer-Fenster auf **Datei | Sitzungsmeldungen speichern.**
2. Geben Sie wie im Dialogfeld "Speichern unter" einen Dateinamen ein und speichern Sie die Datei im Format .TXT. Die Sitzungsmeldungen werden standardmäßig im Ordner **Eigene Dateien** gespeichert.

Fernausführung von Programmen

Sie können im Viewer-Fenster jedes Programm auf einem Fernclient starten. Unter anderem können Sie folgende Aktionen durchführen:

- Ausführung von Diagnosewerkzeugen von der Managementkonsole ausgehend
- Hilfestellung für den Benutzer des Fernclients

So führen Sie Programme entfernt aus

1. Klicken Sie im Viewer-Fenster auf das Menü **Ansicht**. Stellen Sie sicher, dass die Option **Fernausführung** aktiviert ist.
2. Geben Sie im Feld "Ausführen" der Symbolleiste den Pfad für das auszuführende Programm ein. Wenn Sie zum Programm navigieren müssen, klicken Sie auf das Symbol "Durchsuchen" links neben dem Feld.
3. Zur Ausführung des Programms auf dem Fernclient klicken Sie auf das Symbol Fernausführung links neben dem Feld "Ausführen".

Chat mit Fernclients

Sie können das Fenster "Remote Control Viewer" verwenden, um mit einem Benutzer auf einem Fernclient zu chatten. Diese Funktion ist dann hilfreich, wenn Sie einem Fernbenutzer Anweisungen geben müssen, dessen Wählverbindung die einzige verfügbare Telefonleitung verwendet. Der Benutzer kann antworten, indem er das Chat-Fenster nutzt, das auf seinem Bildschirm angezeigt wird. Sie können Chat nur auf Clients verwenden, auf denen der Fernsteuerungsagent installiert ist. Diese Funktion funktioniert auch dann, wenn Sie zur Zeit keinen Client fernsteuern.

Wenn Sie die Nachrichten einer Chat-Sitzung speichern möchten, so können Sie dies tun. Sämtlicher Text, der im grauen Bereich der Chat-Sitzung angezeigt wird, kann in einer Textdatei gespeichert werden.

So chatten Sie mit einem Benutzer an einem Fernclient

1. Geben Sie im Bearbeitungsfeld oben im Viewer-Fenster den Namen eines Clients ein.
2. Klicken Sie auf **Extras | Chat**. Ein Abschnitt des Viewer-Fensters wird zum Chat-Bereich.
3. Geben Sie im Abschnitt unten links des Chat-Bereichs eine kurze Nachricht ein. Klicken Sie auf **Senden**.

Ihre Nachricht wird auf dem Bildschirm des Fernclients angezeigt. Der Benutzer kann antworten, indem er eine Nachricht eingibt und auf **Senden** klickt. Er kann auch auf **Schließen** klicken, um die Chat-Sitzung zu beenden.

So speichern Sie Nachrichten aus einer Chat-Sitzung

1. Klicken Sie im Chat-Bereich des Viewer-Fensters auf **Speichern**.
2. Geben Sie wie im Dialogfeld "Speichern unter" einen Dateinamen ein und speichern Sie die Datei im Format .TXT. Die Chat-Sitzung wird standardmäßig im Ordner **Eigene Dateien** gespeichert.

Übertragen von Dateien auf Fernclients

Mithilfe des Remote Control Viewer-Fensters können Sie Dateien zwischen Ihrem Client und dem Fernclient übertragen. Dies funktioniert im Wesentlichen genauso, als hätten Sie ein Netzlaufwerk verbunden. Sie können nur Dateien zwischen Clients übertragen, auf denen der Fernsteuerungsagent installiert ist. Diese Funktion funktioniert auch dann, wenn Sie zur Zeit keinen Client fernsteuern.

So übertragen Sie Dateien an einen Client

1. Geben Sie im Bearbeitungsfeld oben im Viewer-Fenster den Namen eines Clients ein.
2. Klicken Sie auf **Extras | Dateiübertragung**. Der Windows Explorer wird angezeigt.
3. Wählen Sie eine zu übertragende Datei aus, indem Sie auf ihren Dateinamen klicken. Klicken Sie mit der rechten Maustaste wählen Sie **Kopieren**.
4. Blättern Sie im Baum des Windows Explorers nach unten, bis Sie zu **Ferncomputer** gelangen. Hier sollte der Name des Fernclients angezeigt werden, den Sie zur Zeit steuern.
5. Wählen Sie auf dem Fernclient einen Ordner, in den die Datei eingefügt werden soll, klicken Sie mit der rechten Maustaste und wählen Sie **Einfügen**.

Auf gleiche Weise können Sie Dateien von einem Fernclient auf Ihren Client übertragen.

So konfigurieren Sie die Dateitransfereinstellungen

1. Klicken Sie auf **Extras | Dateiübertragung**. Der Windows Explorer wird angezeigt.
2. Klicken Sie auf **Ferncomputer | Einstellungen**. Das Dialogfeld "Dateitransfereinstellungen" wird angezeigt, es verfügt über die Registerkarten "Allgemein" und "Sitzungsprotokoll".

3. Wählen Sie auf der Registerkarte "Allgemein" eine der folgenden Optionen: "Aktuelle Symbole anzeigen", "Dateisystemänderungen überwachen", "Datenkomprimierung verwenden" und "Netzwerkfreigaben anzeigen".
4. Wählen Sie auf der Registerkarte "Sitzungsprotokoll" eine der folgenden Optionen: "Kopiervorgänge protokollieren", "Löschvorgänge protokollieren", "Verzeichniserstellungsvorgänge protokollieren" und "Umbenennungsvorgänge protokollieren".

Wenn Sie die Registerkarte "Sitzungsprotokoll" wählen und die Sitzungsprotokollvorgänge konfigurieren, wird für diese Vorgänge kein Protokoll gepflegt. Stattdessen werden diese Vorgänge (die gespeichert werden können) im Sitzungsmeldungsbereich des Remote Control Viewer-Fensters aufgezeichnet.

Herunterfahren und Neustarten von Fernclients

Sie können Clients aus der Ferne herunterfahren oder neu starten. Wenn Sie dies tun, wird auf dem Client eine Warnmeldung angezeigt, die dem Benutzer mitteilt, dass das System in 10 Sekunden heruntergefahren wird. Er kann auf die Schaltfläche "Herunterfahren" oder "Abbrechen" klicken. Wenn der Benutzer weder auf "Herunterfahren" noch auf "Abbrechen" klickt, erfolgt das Herunterfahren bzw. der Neustart nach Ablauf der angezeigten Zeit.

Wenn auf dem Client Anwendungen mit ungespeicherten Daten geöffnet sind, werden diese Anwendungen den Abschaltprozess vermutlich unterbrechen und den Benutzer zum Speichern auffordern. Sie müssen den Client ggf. fernsteuern und Anwendungen speichern/schließen bzw. den Benutzer auffordern, dies zu tun, damit das Herunterfahren oder der Neustart erfolgreich durchgeführt werden kann.

So fahren Sie einen Client herunter

- Klicken Sie in der Netzwerkansicht auf den Client, den Sie herunterfahren möchten. Klicken Sie im Kurzbefehlmenü des Clients auf **Herunterfahren**.

So starten Sie einen Client neu

- Klicken Sie in der Netzwerkansicht auf den Client, den Sie neu starten möchten. Klicken Sie im Kurzbefehlmenü des Clients auf **Neustart**.

Konfiguration der Sitzungsoptionen

Verwenden Sie die Elemente unter dem Menü "Optionen", um die Qualität einer Fernsteuerungssitzung zu steigern. Sie können die Anzeigerate erhöhen und die Einstellungen im Viewer-Fenster mit diesen Optionen ändern.

- **Autoscroll:** Aktiviert die Scrollfunktion im Viewer-Fenster, wenn Sie den Cursor an den Fensterrand bewegen. Je dichter Ihr Cursor an den Rand gelangt, umso schneller ist der Scrollvorgang. Aktivieren/Deaktivieren; das Element ist aktiviert, wenn neben diesem im Menü ein Häkchen angezeigt wird.
- **Hotkey-Einstellungen:** Ermöglicht Ihnen, schnell allgemeine Aufgaben zu erledigen, die mit der Fernsteuerung verbunden sind, z. B. Aktualisieren oder Neustarten des Viewer-Fensters.
- **Leistungseinstellungen:** Beschleunigt eine Fernsteuerungssitzung, indem die Farben und Bilder reduziert werden, die vom Bildschirm des Fernclients übertragen werden.
- **Leerer Clientbildschirm:** Leert den Bildschirm des Clients, sodass nur der Benutzer, der den Viewer ausführt, die Benutzerschnittstellenanzeige auf dem Fernclient sehen kann. Aktivieren/Deaktivieren; das Element ist aktiviert, wenn neben diesem im Menü ein Häkchen angezeigt wird.
- **Tastatur und Maus sperren:** Sperrt Tastatur und Maus des Clients, sodass nur der Benutzer, der das Viewer-Fenster ausführt, den Fernclient steuern kann. Aktivieren/Deaktivieren; das Element ist aktiviert, wenn neben diesem im Menü ein Häkchen angezeigt wird.
- **Zwischenablagen synchronisieren:** Synchronisiert die Tastaturen zwischen Verwaltungskonsole und Fernclient, sodass Sie Informationen von beiden Clients einfügen können. Aktivieren/Deaktivieren; das Element ist aktiviert, wenn neben diesem im Menü ein Häkchen angezeigt wird.

So konfigurieren Sie Sitzungsoptionen

1. Klicken Sie im Viewer-Fenster auf das Menü **Optionen**.
2. Klicken Sie auf die Optionen, die Sie aktivieren oder konfigurieren möchten.

Anpassen der Anzeigeoptionen

Da Remote Control Viewer-Fenster verfügt über diverse Anzeigeoptionen, die Sie für eine Fernsteuerungssitzung anpassen können.

- **Symbolleiste:** Zeigt Symbole für die Elemente aus dem Menü "Extras" an.
- **Statusleiste:** Wird ganz unten im Viewer-Fenster angezeigt. Zeit den Status von Vorgängen im Viewer-Fenster.
- **Sitzungsmeldungen:** Werden im unteren Bereich des Viewer-Fensters angezeigt. Diese Meldungen zeigen Ihnen genau, was passiert ist, während das Viewer-Fenster geöffnet war. Sie können bei der Fehlerkorrektur behilflich sein, wenn Sie keine Verbindung mit einem Fernclient herstellen können. Sie können diese Meldungen in einer .TXT-Datei speichern, um sie sich später erneut anzusehen.

- **Fernausführung:** Zeigt die Fernausführungssteuerungen in der Symbolleiste an, mit denen Sie eine Batch-Datei oder Anwendung auf dem Fernclient suchen und ausführen können.

So passen Sie die Anzeigeoptionen an

1. Klicken Sie im Viewer-Fenster auf das Menü **Ansicht**.
2. Aktivieren oder deaktivieren Sie die Optionen. Sie können beliebig viele Optionen gleichzeitig aktivieren. Alle Einstellungen werden sofort übernommen und werden bei der nächsten Fernsteuerungssitzung beibehalten.

Informationen zu Fernsteuerungs-Hotkeys

Mithilfe von Hotkeys können Sie schnell die Aufgaben ausführen, die während der Fernsteuerung häufig verwendet werden. Es sind bereits Standard-Hotkey-Einstellungen vorhanden, aber Sie können diese an Ihre Anforderungen anpassen. Hotkeys sind standardmäßig aktiviert.

- **Ansicht aktualisieren:** Aktualisiert das Viewer-Fenster.
- **Ansicht neu starten:** Aktualisiert das Viewer-Fenster und die Daten auf dem Bildschirm des Fernclients.
- **Hotkeys aktivieren:** Aktiviert oder deaktiviert die in diesem Dialogfeld konfigurierten Hotkeys. Wenn Sie die Einstellung ändern, wird die Meldung "Hotkeys: Aktiviert/Deaktiviert" im Viewer-Fenster angezeigt.
- **Anzeigesitzung beenden:** Schließt die Fernsteuerungssitzung mit einem bestimmten Client.

So ändern Sie die Hotkey-Einstellungen

1. Klicken Sie im Viewer-Fenster auf **Optionen | Hotkey-Einstellungen**.
2. Platzieren Sie den Cursor im Bearbeitungsfeld der Hotkey-Einstellung, die Sie ändern möchten. Die Tastenkombinationen mit Strg+Alt funktionieren am besten, da sie vermutlich noch nicht in anderen Anwendungen belegt sind.
3. Drücken Sie auf Ihrer Tastatur die neue Hotkey-Tastenkombination, die Sie verwenden möchten. Die Tastenkombination wird als neue Einstellung angezeigt.
4. Klicken Sie auf **OK**, um die Änderung zu übernehmen.

So deaktivieren Sie eine Hotkey-Einstellung

1. Klicken Sie im Viewer-Fenster auf **Optionen | Hotkey-Einstellungen.**
2. Platzieren Sie den Cursor im Bearbeitungsfeld der Hotkey-Einstellung, die Sie deaktivieren möchten.
3. Drücken Sie auf der Tastatur die Taste **Löschen**. Im Bearbeitungsfeld wird "Keine" angezeigt.
4. Klicken Sie auf **OK**, um die Änderung zu übernehmen.

So verwenden Sie Hotkeys

1. Für die Verwendung von Hotkeys müssen Sie einen Client aktiv fernsteuern.
2. Drücken Sie im aktiven Viewer-Fenster die Hotkey-Tastenkombination für eine der verfügbaren Aktionen.

Informationen zum Viewer-Fenster-Fokus...
Sollten Sie feststellen, dass die Hotkeys nicht funktionieren, könnte dies daran liegen, dass das Viewer-Fenster nicht das aktive Fenster ist. Wenn der Rahmen blau/schwarz ist, ist das Fenster nicht aktiv. Klicken Sie mit dem Cursor in das Fenster, sodass sich der Rahmen in gelb/schwarz ändert. Sie sollten nun Hotkeys verwenden können.

Informationen zu den Einstellungen der Fernsteuerungsleistung

Die Leistungseinstellungen beschleunigen eine Fernsteuerungssitzung auf Fernclients. Wenn die Anzeigerate zu langsam ist, können Sie eine Komprimierungsmethode wählen, um den Overhead zu verringern. Die Komprimierungsmethoden sind standardmäßig deaktiviert.

- **Clienthintergrundbild unterdrücken:** Erhöht die Anzeigerate, in dem der Hintergrund des Fernclients unterdrückt wird. Aufwändige Hintergrundbilder können die Geschwindigkeit einer Fernsteuerungssitzung erheblich beeinträchtigen.
- **JPEG-Komprimierung:** Wenn Sie einen Client fernsteuern, der Bitmaps anzeigt, ersetzt diese Option effizient den Bedarf für eine Unterdrückung des Client-Hintergrundbildes durch die Komprimierung großer Bilder. Dies eignet sich auch für große Splash-Bildschirme. Bei dieser Option kann es einige Bildartefakte geben, z. B. wenn Sie den Cursor über ein Bitmap-Bild bewegen. Funktioniert bei Windows NT-/2000-/2003-/XP-Fernclients.
- **Reduzierung der Farbtiefe:** Wenn Sie eine Verbindung über eine langsame Verbindung oder über eine Dial-UP-Netzwerkverbindung herstellen, verringert diese Option die Anzahl der übertragenen Farboptionen. Je dichter Sie an die vollständige Reduzierung gelangen, umso mehr Farbartefakte sehen Sie. Funktioniert bei Windows NT-/2000-/2003-/XP-Fernclients.

So aktivieren Sie die Kompressionsmethoden

1. Klicken Sie im Viewer-Fenster auf **Optionen | Leistungseinstellungen.**
2. Klicken Sie auf **Clienthintergrundbild unterdrücken**, wenn Sie die Anzeigerate erhöhen möchten.
3. Verschieben Sie für die **JPEG-Komprimierung** den Regler in Richtung **Vollständige Kompression**, um die höchste Bildkomprimierung und Anzeigerate zu erzielen.
4. Verschieben Sie für die **Reduzierung der Farbtiefe** den Regler in Richtung **Vollständige Reduzierung**, um die höchste Farbreduzierung und Anzeigerate zu erzielen.

Ändern der Client-Fernsteuerungssicherheit

Management Suite kann die Clients mit Zugriffsrechten weitreichend steuern. Der Client steuert die Fernzugriffssicherheit. Er speichert seine Sicherheitseinstellungen für den Fernzugriff in der Registrierung.

Der Benutzer kann in den Fernsteuerungseinstellungen festlegen, dass jedem Zugriff gewährt werden soll, der versucht, den Client fernzusteuern. Wenn eine Konsole versucht, einen solchen Client fernzusteuern, wird auf dem Clientbildschirm eine Meldung angezeigt. Diese gibt den Namen des Konsolenbenutzers an und bittet um Fernsteuerungszugriff. Hierdurch erfolgt eine einfache Authentifizierung zwischen Verwaltungskonsole und Client.

Wenn Sie Windows NT-/2000-/2003-/XP-Clients fernsteuern, liefert Management Suite über den Benutzer-Manager zusätzliche Sicherheitsfunktionen, indem nur bestimmten Viewers Fernzugriff gewährt wird.

Weitere Informationen zur Fernsteuerungssicherheit und zu Clientkonfigurationen finden Sie unter Verteilen der Fernsteuerung in Kapitel 2.

So ändern Sie die Sicherheitseinstellungen eines Clients

1. Klicken Sie in der Windows-Taskleiste oder während der Steuerung eines Clients auf **Start** | **Programme** | **LANDesk Management** | **Fernsteuerungseinstellungen**.
2. Klicken Sie auf die gewünschten **Einstellungen**.
3. Klicken Sie auf **Übernehmen**, damit die neuen Sicherheitseinstellungen sofort wirksam werden.
4. Klicken Sie auf **OK**.

Sie können die Fernsteuerungseinstellungen auch bearbeiten, indem Sie das Programm EDITINI.EXE von der Befehlszeile des Betriebssystems ausführen. Wenn Sie die Sicherheitseinstellungen für einen Windows NT-/2000-/2003-/XP-Client ändern, sollten Sie sicherstellen, dass Sie als Administrator in der Fernsteuerungsoperatoren-Gruppe enthalten sind.

Konfigurieren der Mac OS X-Fernsteuerungsoptionen

Der Mac OS X-Fernsteuerungs-Clientagent verfügt über Optionen, die denen auf Windows-Clients ähneln. Sie können die folgenden Fernsteuerungsoptionen konfigurieren:

- **Anwendungen und Dateien öffnen:** Erlauben Sie einem Administrator, Dateien auf diesem Client aus der Ferne zu öffnen.
- **Elemente kopieren:** Erlauben Sie einem Administrator, aus der Ferne Dateien von und auf diesen Client zu kopieren.
- **Elemente löschen und umbenennen:** Erlauben Sie einem Administrator, aus der Ferne Dateien auf diesem Client zu löschen oder umzubenennen.
- **Tastatur und Maus sperren:**Erlauben Sie einem Administrator, Ihre Tastatur und Maus während einer Fernsteuerungssitzung zu sperren. Diese Option verhindert, dass Sie Fernvorgänge behindern.
- **Leerer Bildschirm:** Erlauben Sie einem Administrator, Ihren Bildschirm während einer Fernsteuerungssitzung zu leeren. Diese Option ist dann hilfreich, wenn sich auf Ihrem Client sensitive Dokumente befinden, die ein Administrator ggf. aus der Ferne öffnen muss. Mit dieser Option verhindern Sie, dass vorbeikommende Personen diese Dokumente lesen können.
- **Neu starten und herunterfahren:**Erlauben Sie einem Administrator, Ihren Client aus der Ferne neu zu starten oder herunterzufahren.
- **Steuern und überwachen:**Erlauben Sie einem Administrator, Ihre Aktionen auf diesem Client zu steuern und zu überwachen.
    - **Überwachung anzeigen:** Wenn eine Fernsteuerungssitzung aktiv ist, wird in der Menüleiste ein sichtbares Symbol angezeigt (nur OS X).
- **Steuerung an Benutzer abgeben:**Erlauben Sie einem Administrator, diesen Client in folgenden Situationen fernzusteuern:
    - **Immer:** Von jeder Domäne, wann immer notwendig.
    - **Aus gleicher Domäne:**Nur aus der gleichen Domäne.
    - **Nach Sitzung:** Von Sitzung zu Sitzung. Jedes Mal, wenn der Administrator versucht, eine Fernsteuerungssitzung aufzunehmen, wird ein Dialogfeld angezeigt, über das Sie die Sitzung zulassen oder verhindern können.
- **Tiefe:** Wählen Sie die an das Remote Control Viewer-Fenster in der Konsole oder Webkonsole zu übertragende Farbtiefe. Je höher die Farbtiefe, umso mehr Bandbreite wird für die Fernsteuerung benötigt und verbraucht. Zu Beginn einer Fernsteuerungssitzung ändert sich die Farbtiefe in den gewählten Wert.

So konfigurieren Sie Mac OS X Fernsteuerungsagent-Einstellungen

1. Öffnen Sie auf dem Macintosh OS X-Client die **Systemvoreinstellungen** und wählen Sie den Bereich **LANDesk® Management Suite-Client**.
2. Leben Sie auf der Registerkarte **Fernsteuerung** Ihre Einstellungen fest.

Verwenden der Fernsteuerungsprotokollierung

Management Suite protokolliert standardmäßig Fernsteuerungsaktionen, einschließlich des Clients, der ferngesteuert wird, und der Konsole, die die Fernsteuerung ausführt. Sie können die Fernsteuerungsprotokollierung deaktivieren oder Fernsteuerungsprotokolleinträge löschen, die älter als ein angegebenes Datum sind. Wenn die Protokollierung aktiviert ist, können Sie die folgenden Fernsteuerungsberichte anzeigen (**Extras | Berichte > Alle Fernsteuerungsberichte**):

- Fernsteuerungsverlauf nach Client
- Fernsteuerungsverlauf nach Konsole
- Fernsteuerungsverlauf nach verwaltete Computer
- Fernsteuerungsübersicht

So aktivieren oder deaktivieren Sie die Fernsteuerungsprotokollierung

1. Klicken Sie auf **Konfigurieren | Fernsteuerungsprotokollierung**.
2. Aktivieren oder deaktivieren Sie je nach Präferenz die Option **Fernsteuerungsprotokollierung aktivieren**.

So löschen Sie den Inhalt des Fernsteuerungsprotokolls

1. Klicken Sie auf **Konfigurieren | Fernsteuerungsprotokollierung**.
2. Geben Sie das Datum ein, das Sie löschen möchten. Alle Einträge, die älter sind als dieses Datum, werden gelöscht.
3. Klicken Sie auf **Jetzt tilgen**, um die Einträge aus dem Protokoll zu löschen.

Fehlerkorrektur bei Fernsteuerungssitzungen

Dieser Abschnitt beschreibt mögliche Probleme bei der Fernsteuerung eines Clients und liefert mögliche Lösungen.

Ich kann einen Client nicht fernsteuern

Überprüfen Sie, ob auf dem Client die LANDesk-Agenten geladen sind.

So überprüfen Sie, ob die LANDesk-Agenten geladen sind:

- Klicken Sie in der Netzwerkansicht der Konsole auf **Eigenschaften** im Kontextmenü des Clients. Klicken Sie auf die Registerkarte **Agenten** und zeigen Sie die geladenen Agenten an.

So laden Sie den Fernsteuerungsagenten

- Erstellen Sie einen Clientkonfigurationstask in der Konsole und verteilen Sie ihn mittels Push-Vorgang auf den Client. Alternativ dazu können Sie auch ein Laufwerk auf dem Client dem Core Server zuordnen und den entsprechenden Clientkonfigurationstask ausführen.

Das Remote Control Viewer-Fenster weist schwarze Flecken oder fehlende Zeichen auf

Dieses Problem ist in der Regel auf eine Inkompatibilität mit dem Videotreiber zurückzuführen.

So lösen Sie die Inkompatibilität mit Videotreibern

1. Holen Sie sich den neuesten Videotreiber vom Hersteller.
2. Stellen Sie sicher, dass Sie über die neuesten LANDesk-Agenten und Anzeigetreiber verfügen.

Die Images vom Ziel-Client werden nicht korrekt im Remote Control Viewer-Fenster angezeigt

Dieses Problem ist in der Regel auf eine Inkompatibilität mit dem Videotreiber zurückzuführen.

So lösen Sie die Inkompatibilität mit Videotreibern

1. Holen Sie sich den neuesten Videotreiber vom Hersteller.
2. Stellen Sie sicher, dass Sie über die neuesten LANDesk-Agenten und Anzeigetreiber verfügen.

Kein Dateitransfer zwischen Konsole und Ziel-Client möglich

Überprüfen Sie, ob Norton AntiVirus* ausgeführt wird und ob Integrity Shield aktiviert ist. Wenn Integrity Shield aktiviert ist, benötigen Sie vorübergehende Rechte, um in das Verzeichnis kopieren zu können, das von Integrity Shield geschützt wird.

Der Ziel-Client hängt bzw. eine andere Anwendung funktioniert nicht, nachdem LANDesk-Agenten geladen wurden

Dieses Problem kann durch Konflikte zwischen Management Suite und anderen Fernzugriffsanwendungen verursacht werden.

So lösen Sie Konflikte zwischen Management Suite und anderen Anwendungen

1. Holen Sie sich die neueste Softwareversion vom Hersteller.
2. Stellen Sie sicher, dass Sie über die neuesten LANDesk-Agenten verfügen.

Kapitel 6: Verteilen von Software und Dateien

In diesem Kapitel wird beschrieben, wie mithilfe von LANDesk Management Suite Software und Dateien an Clients in einem Netzwerk verteilt werden.

In diesem Kapitel erfahren Sie mehr über:

- Enhanced Software Distribution
- Verwenden von Targeted Multicast mit Enhanced Software Distribution
- Einrichten eines Paketerstellungscomputers
- Übersicht über die Paketerstellung
- Ausführen des Package Builder-Assistenten
- Einrichten des Übermittlungsservers
- Konfigurieren von Clients für den Empfang von Paketen
- Verteilen eines Pakets
- Checkpunkt-Neustarts auf Byte-Ebene und dynamische Bandbreitendrosselung
- Arbeiten mit Mac OS X-Verteilungsskripten und -paketen
- Verteilen von Dateien mit einem Dateiübertragungsskript
- Deinstallieren von Softwareverteilungspaketen

Enhanced Software Distribution

Mit Enhanced Software Distribution (ESWD) können Sie Software- und Dateipakete für Clients bereitstellen, auf denen folgende Betriebssysteme ausgeführt werden:

- Windows 95B/98SE
- Windows NT (4.0 SP6a und höher)
- Windows 2000/2003/XP
- Mac OS X 10.2.x. und 10.3.x

Folgende Funktionen sind für die Softwareverteilung verfügbar:

- Funktionen von LANDesk Targeted Multicasting™, die bei der Verteilung umfangreicher Pakete an viele Benutzer den Bandbreitenverbrauch minimieren, ohne dedizierte Hardware oder eine Neukonfiguration der Router zu erfordern.
- Skripte für Verteilungsaufgaben ermöglichen eine detaillierte Steuerung der Art und Weise, in der Tasks ausgeführt werden
- Einfacher Task-Scheduler arbeitet mit der Inventardatenbank zusammen, um die Auswahl der Ziele zu erleichtern
- Echtzeit-Statusberichte für jeden Verteilungs-Task
- Verteilung an Macintosh* OS 10.2-Clients
- Unterstützung mobiler Geräte, einschließlich Bandbreitenerkennung, Checkpoint-Neustarts und automatische Erledigung von Tasks
- Package Builder mit vollem Funktionsumfang
- Verteilung beliebiger Pakettypen, einschließlich MSI, setup.exe und anderer Installationsprogramme
- Push- und Pull-Verteilung zur Unterstützung Ihrer Verteilungsstrategien

ESWD verwendet Paketerstellungstechnologie, um ein eigenständiges ausführbares Programm für die erforderliche Softwareinstallation zu erstellen. Sobald ein Paket erstellt ist, wird es auf einem Web- oder Netzwerkserver gespeichert, der als "Übermittlungsserver" bezeichnet wird. Über die Konsole können Sie die Verteilung mithilfe des Scheduler planen. Der Core Server kommuniziert den Speicherort des Pakets (URL) an den Client und kopiert dann nur die Dateien vom Übermittlungsserver, die der Client benötigt.

Wenn Sie beispielsweise ein Softwareprogramm neu installieren, weil einige Dateien beschädigt sind oder fehlen, werden vom System nur die beschädigten bzw. fehlenden Dateien kopiert, nicht das ganze Programm. Diese Technologie funktioniert auch über WAN-Verbindungen. Sie können das Paket auf mehreren Servern speichern und festlegen, dass die Clients jeweils auf den Server zugreifen, der für ihre Anforderungen (d. h. in Bezug auf Standort, Nähe, Bandbreitenverfügbarkeit usw.) am besten geeignet ist.

ESWD nimmt zudem unterbrochene Download-Vorgänge für Pakete wieder auf. Wenn beispielsweise ein mobiler Client gerade ein umfangreiches Paket heruntergeladen hat, als seine Netzwerkverbindung getrennt wurde, wird der Ladevorgang nach der Wiederherstellung der Verbindung genau an der Stelle fortgesetzt, an der er unterbrochen wurde.

In den folgenden Schritten wird die Softwareverteilung beschrieben:

1. Installieren Sie die Package Builder-Software.
2. Erstellen Sie ein Softwarepaket.
3. Stellen Sie das Paket auf dem Übermittlungsserver bereit, damit es an die Clients gesendet werden kann.
4. Wählen Sie mithilfe der Konsole ein Paket aus, das auf den Clients installiert werden soll, und konfigurieren Sie einen Task zur Bereitstellung dieses Pakets.
5. Planen Sie die Übermittlung des Pakets an die Clients.
6. Sobald der geplante Zeitpunkt erreicht ist, kontaktiert der Scheduler den ESWD-Agenten auf den einzelnen Clients und informiert ihn darüber, dass das Paket zur Installation bereit ist.
7. Der ESWD-Agent lädt das Paket vom Übermittlungsserver herunter und verarbeitet es auf dem Client, indem er die verpackten Dateien installiert oder entfernt.
8. Nach der Verarbeitung des Pakets sendet der ESWD-Agent das Ergebnis an den Core Server, wo es in die Core-Datenbank eingefügt wird.

Folgende Komponenten der Softwareverteilung befinden sich auf dem Core Server bzw. werden darauf ausgeführt:

- **LANDesk Benutzerdefinierte Autragsverwaltung:** Dieses vom Scheduler gestartete Programm (CUSTJOB.EXE) initiiert einen Verteilungsauftrag.
- **LANDesk Scheduler-Dienst:**Die Konsole kommuniziert mit diesem Programm (SCHEDSVC.EXE), um die Paketverteilung zu planen.
- **Verteilungspaketskript:** Diese kleine .INI-Skriptdatei wird erstellt, wenn Sie im Fenster "Skripts verwalten" ein Softwareverteilungspaket auswählen. Die Skriptdatei wird an Clients gesendet. Diese verwenden die Befehle im Skript zum Herunterladen und Installieren des Pakets.
- **Softwareverteilungspakete:** Diese Pakete erstellen Sie auf dem Paketerstellungscomputer, sie werden jedoch nicht automatisch auf den Übermittlungsserver verschoben.

Verwenden von Targeted Multicast mit Enhanced Software Distribution

Die LANDesk Targeted Multicast-Technologie ermöglicht es, mit einem minimalen Aufkommen an Netzwerkverkehr umfangreiche Pakete über das Netzwerk an viele Benutzer zu verteilen. Targeted Multicast-Funktionen erfordern weder zusätzliche Hardware- oder Software-Infrastruktur noch spezielle Router-Konfigurationen für das Versenden von Multicast-Paketen. Sie erhalten die außerordentlichen Vorteile der Multicast-Technologie ohne die sonst üblichen Probleme.

Targeted Multicast funktioniert mit den vorhandenen Softwareverteilungspaketen. Wenn Sie Targeted Multicast verwenden, ist das Verteilen der Software ganz einfach, selbst in WAN-Umgebungen mit mehreren Hops und niedrigen Verbindungsgeschwindigkeiten (56 KBit/s). Targeted Multicast verwendet HTTP für die Übermittlung von einer Website an einen Subnetzrepräsentanten. Der Management Suite-Inventarscanner stellt dem Targeted Multicast-Dienst alle Subnetzinformationen zur Verfügung.

Targeted Multicast bietet zahlreiche Vorteile, die Standard-Multicast-Methoden nicht aufweisen. Mithilfe der inventarbasierten Angabe von Clients können Sie ein Paket über ein Multicast an eine ausgewählte Gruppe von Computern senden, die bestimmte Kriterien erfüllen. Mit Targeted Multicast wird das Verfahren auch deshalb vereinfacht, weil Router nicht extra für die Verarbeitung von übermittelten Paketen konfiguriert werden müssen.

Verglichen mit konventionellen Softwareverteilungsmethoden wird bei der Übermittlung von Softwarepaketen mit Targeted Multicast deutlich weniger Zeit und Bandbreite benötigt. Statt für jeden Client ein Paket über das Netzwerk zu senden, wird für jedes Subnetz nur eine Übertragung durchgeführt. Je höher die Anzahl der Clients in jedem Subnetz, desto mehr Bandbreite wird eingespart.

Wenn Sie Targeted Multicast aktivieren möchten, wählen Sie die Option **Dieses Paket mit Multicast verteilen** im Dialogfeld "Skript erstellen" aus, das beim Erstellen eines Verteilungspaketskripts angezeigt wird. Mit der Aktivierung dieser Option werden zusätzliche multicast-spezifische Seiten dem Skripterstellungs-Assistenten hinzugefügt.

Wenn Sie eine Verteilung mithilfe von Targeted Multicast starten, wird das Fenster "Multicast Software Distribution" angezeigt. Dieses Fenster enthält ausführliche Informationen zum Verteilungsvorgang. Weitere Informationen zur Bedeutung der einzelnen Felder erhalten Sie, wenn Sie im Fenster "Multicast Software Distribution" auf die Schaltfläche **Hilfe** klicken.

Sowohl Windows- als auch Macintosh OS 10.2-Clients unterstützen Targeted Multicast.

Verwenden von Peer Download

Management Suite 8 ergänzt Targeted Multicast durch die neue Funktion Peer Download. Peer Download zwingt Zielclients, ein Paket aus ihrem lokalen Cache oder von einem Peer im gleichen Subnetz zu installieren. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Paketinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sich das Paket im lokalen Cache oder im Cache eines Peer des Clients befindet. Eine Möglichkeit zur Nutzung dieser Option besteht darin, das Paket zuerst mit der Option **Dateien mit Multicast an lokales Multicast-Cache-Verzeichnis verteilen**, die an früherer Stelle im Assistenten verfügbar ist, auf einen Client in jedem Subnetz zu kopieren.

Auch wenn Sie die Option **Peer Download** nicht auswählen, versucht der Targeted Multicast-Clientagent, Bandbreite zu sparen, indem er die folgenden Speicherorte in der unten angegebenen Reihenfolge nach Paketdateien überprüft:

1. Lokaler Cache
2. Peer im gleichen Subnetz
3. Paketserver

Kopieren von Dateien in den Multicast-Ordner im lokalen Cache

Sie können eine oder mehrere Dateien mithilfe von Multicast in den Multicast-Ordner im lokalen Cache kopieren. Mit dieser Option wird eine Datei in den lokalen Cache der Clients kopiert. Die Datei wird damit nicht installiert oder in irgendeiner anderen Weise verarbeitet. Diese Option erleichtert es, Dateien auf Multicast-Domänenrepräsentanten oder Clients in den verschiedenen Multicast-Domänen bereitzustellen. Sie können die Dateien zuerst an die Domänenrepräsentanten verteilen und die Verteilung danach mit der Option "Peer Download" wiederholen, um sicherzustellen, dass die Clients die Pakete nur von einem Peer in ihrem Subnetz herunterladen.

Konfigurieren von Targeted Multicast

Bevor Sie Targeted Multicast verwenden können, müssen Sie sicherstellen, dass sich die Targeted Multicast-Komponenten in dem Subnetz befinden, an das die Pakete verteilt werden sollen. Targeted Multicast erfordert Management Suite 8-Agenten und Multicast-Domänenrepräsentanten.

Um die Multicasts zu reduzieren, ändern Sie die Option **Mindestanzahl der Millisekunden zwischen Paketübertragungen** im Dialogfeld **Erweiterte Multicast-Optionen konfigurieren** des **Migrationstasks-Assistenten**.

So geben Sie manuell an, welche Computer als Multicast-Domänenrepräsentanten verwendet werden sollen

1. Klicken Sie in der Netzwerkansicht auf **Konfiguration > Multicast-Domänenrepräsentanten**.
2. Fügen Sie Domänenrepräsentanten hinzu, indem Sie die Computer, die als Repräsentanten fungieren sollen, von der Netzwerkansicht in diese Kategorie ziehen.

Targeted Multicast verwendet den ersten Computer jedes Subnetzes aus der Gruppe "Multicast-Domänenrepräsentanten", der antwortet.

Nur Windows-Computer können als Multicast-Domänenrepräsentanten fungieren. Wenn Sie Pakete über Targeted Multicast an Macintosh-Computer verteilen möchten, müssen Sie sicherstellen, dass zur Multicast-Domäne mindestens ein Windows-Computer gehört, der für die Macintosh-Computer als Domänenrepräsentant dienen kann. Wenn in einer Umgebung, in der Macintosh-Computer vorherrschen, nur einige wenige Windows-Computer vorhanden sind, sollten Sie die Windows-Domänenrepräsentanten in der Gruppe "Multicast-Domänenrepräsentanten" manuell festlegen.

Infos über das Register "Management Suite-Dienste"

Sie können die Targeted Multicast-Optionen im Dialogfeld "Management Suite-Dienste konfigurieren" auch anpassen.

Um den Targeted Multicast-Dienst zu konfigurieren, klicken Sie auf das Register **Konfigurieren | Dienste | Multicast**.

- **Multicast-Domänenrepräsentanten:** Verwendet alle Domänenrepräsentanten, die in der Gruppe **Konfiguration > Multicast-Domänenrepräsentanten** der Netzwerkansicht angegeben wurden.
- **Cachedatei verwenden:**Fragt jede Multicast-Domäne ab, um herauszufinden, wer die Datei bereits besitzt; in diesem Fall wird die Datei nicht auf einen Repräsentanten heruntergeladen.
- **Cachedatei vor bevorzugtem Domänenrepräsentanten verwenden:**Ändert die Reihenfolge der Erkennung, sodass "Cachedatei verwenden" die erste getestete Option zur Auswahl des Domänenrepräsentanten ist.
- **Broadcast verwenden:**Sendet einen Subnetz-Broadcast, um Computer in diesem Subnetz zu finden, die Multicast-Domänenrepräsentanten sein könnten.
- **Verwerfungszeitraum protokollieren:**Legt die Anzahl der Tage fest, die Einträge im Protokoll bis zum Löschen erhalten bleiben.

Falls mit keiner dieser Multicast-Erkennungsmethoden ein Multicast-Repräsentant gefunden werden kann, kontaktiert der Multicast-Server jeden Client in der Zielliste, um zu ermitteln, ob er als Multicast-Repräsentant fungieren kann.

Einrichten eines Paketerstellungscomputers

Bei dem Paketerstellungscomputer sollte es sich um einen dedizierten Computer mit einem neu installierten Betriebssystem handeln. Die Neuinstallation ist erforderlich, weil bei der Paketerstellung alle auf dem Paketerstellungscomputer hinzugefügten oder geänderten Elemente erfasst werden.

Da Pakete nur an Clients verteilt werden können, auf denen dasselbe Betriebssystem wie auf dem Paketerstellungscomputer ausgeführt wird, sollten Sie für jedes Betriebssystem, an das Pakete verteilt werden, einen separaten Paketerstellungscomputer oder eine separate Laufwerkspartition besitzen. Sie können auch einen Computer mit mehreren Betriebssystemabbildern als Paketerstellungscomputer verwenden.

Mit jeder bereits auf dem Paketerstellungscomputer vorinstallierten Software kann Package Builder weniger Änderungen erkennen. Aus diesem Grund sollte möglichst wenig auf dem Paketerstellungscomputer vorinstalliert oder konfiguriert sein, damit er so ursprünglich und "sauber" wie möglich ist. Dies gilt auch für die Dateien CONFIG.SYS und AUTOEXEC.BAT sowie andere Konfigurationsdateien, die unter Umständen beim Installieren der Anwendung geändert werden.

So installieren Sie die Paketerstellungssoftware

1. Suchen Sie vom Paketerstellungscomputer aus die Datei **ENUSETUP.EXE** im Ordner LDMAIN\install\Package_Builder des Core Servers.
2. Doppelklicken Sie auf **ENUSETUP.EXE**, und klicken Sie anschließend auf **Weiter**.
3. Geben Sie den Speicherort des Ordners ein, in dem die Paketerstellungssoftware installiert werden soll, und klicken Sie auf **Fertigstellen**.

Es werden drei Komponenten auf dem Paketerstellungscomputer installiert:

- **Package Builder-Assistent:** Damit werden Softwareverteilungspakete automatisch erstellt. Zunächst wird eine "Vorher"-Statusaufnahme des Computers angefertigt, dann werden Sie aufgefordert, die Software zu installieren. Anschließend erfolgt eine "Nachher"-Statusaufnahme des Computers, und ein Paket mit den Statusunterschieden wird erstellt.
- **Enhanced Package Builder:** Damit werden Softwareverteilungspakete manuell erstellt, geändert und bearbeitet.
- **Hilfe zum Package Builder-Assistenten:** Eine Online-Hilfe, in der die Funktionen des Package Builder-Assistenten beschrieben werden.

Sobald die Package Builder-Software auf dem Computer installiert ist, können auf diesem Computer Softwareverteilungspakete erstellt und bearbeitet werden. Package Builder speichert Pakete standardmäßig auf der lokalen Festplatte. Sobald diese Pakete erstellt sind, müssen Sie sie vom Paketerstellungscomputer auf die Paketfreigabe auf dem Übermittlungsserver verschieben.

Übersicht über die Paketerstellung

Mit dem Package Builder-Assistenten können Sie die Statusaufnahme automatisieren und sie in eigenständige Pakete kompilieren. Wie im Folgenden beschrieben, umfasst der Prozess vier Schritte:

1. Statusaufnahme vor der Installation
2. Installieren der Anwendung oder Ändern der Computerkonfiguration
3. Statusaufnahme nach der Installation
4. Wiederherstellen des Paketerstellungscomputers

1. Statusaufnahme vor der Installation

Um ein Softwarepaket zu erstellen, müssen Sie die lokale Festplatte mit Package Builder scannen. Auf der Seite "Scanoptionen" können Sie genau angeben, welche Bereiche der Festplatte gescannt werden sollen. Bei diesem Scan werden die Systemregistrierung und alle Verzeichnisse und Dateien auf dem lokalen Computer überprüft. Wenn Sie die neue Software auf dem System installiert haben, verwendet Package Builder diese Informationen, um die auf dem Computer vorgenommenen Änderungen zu ermitteln. Anschließend werden diese Änderungen kompiliert und das Softwareverteilungspaket erstellt. Diese Information wird im temporären Arbeitsverzeichnis gespeichert. Geben Sie dieses Verzeichnis auf der Seite "Optionen" des Package Builder-Assistenten an.

Package Builder scannt standardmäßig alle lokalen Laufwerke. Wenn Sie sicher sind, dass ein lokales Laufwerk während der Installation nicht geändert wird, können Sie es für den Scan ausschließen und dadurch die "Vorher"-Statusaufnahme beschleunigen. Die besten Ergebnisse erzielen Sie, wenn Package Builder die Festplattenpartition scannt, auf der das Betriebssystem gespeichert ist, und das Laufwerk, auf dem die Software installiert bzw. die Konfiguration geändert wird.

Wenn bei der Paketerstellung der Speicherplatz auf der Festplatte des Paketerstellungscomputers knapp wird, hält Package Builder an und gibt eine Warnung aus. Sie können zusätzlichen Speicherplatz freigeben und dann mit der Paketerstellung fortfahren.

Selbst wenn alle lokalen Laufwerke aus der Scanliste entfernt werden, scannt Package Builder dennoch die Systemdateien und -ordner sowie die Registrierung des Computers.

2. Installieren der Anwendung oder Ändern der Computerkonfiguration

Sobald die Statusaufnahme vor der Installation abgeschlossen ist, werden Sie von Package Builder aufgefordert, die Anwendungssoftware zu installieren, die als Paket verteilt werden soll.

Sie können mehrere Anwendungen in einem Paket installieren, allerdings sollten Sie mit diesem Prozess nur Suite-Anwendungen installieren. Wenn Sie mehrere Anwendungen als ein Verteilungspaket installieren und später eine davon weglassen möchten, müssen Sie zuerst die ganze Gruppe entfernen und dann eine neue Anwendungsgruppe installieren. Wenn Sie mehrere Pakete auf den verwalteten Clients installieren möchten, bearbeiten Sie das Softwareverteilungsskript so, dass bei der Verteilung mehrere verschiedene Pakete installiert werden.

Package Builder überwacht diesen Schritt der Installation und wartet, bis die Installation abgeschlossen ist, bevor die folgenden Assistentenseiten ausgeführt werden. Anschließend können Sie das fertige Programm anpassen. Wenn das Installationsprogramm beispielsweise ein Deinstallationssymbol erstellt, das Sie nicht an die Clients verteilen möchten, können Sie das Symbol vor der "Nachher"-Sofortaufnahme in Schritt 3 löschen. Es wird dann aus dem Paket entfernt. Sie können für bestimmte Programmgruppen auch neue Symbole hinzufügen, die den Benutzern als zentraler Zugangspunkt dienen.

Sie müssen alle vom System angeforderten Setupinformationen angeben und alle Fragen beantworten, die beim Softwaresetup angezeigt werden. Package Builder kann dies nicht für Sie übernehmen. Die Informationen werden jedoch als Teil des Pakets gespeichert.

Wenn Sie nur einige der Systemeinstellungen auf Clients ändern oder eine Sammlung bestimmter Dateien kopieren möchten, können Sie ein Paket erstellen, ohne eine Statusaufnahme durchführen zu müssen.

Wenn die Installation der Anwendungssoftware bzw. die Konfigurationsänderungen abgeschlossen sind, wechseln Sie zurück zum Assistenten, und klicken Sie auf "Weiter", um die "Nachher"-Statusaufnahme durchzuführen.

3. Statusaufnahme nach der Installation

In diesem Schritt führt Package Builder eine zweite Statusaufnahme des Paketerstellungscomputers durch und vergleicht sie mit der "Vorher"-Statusaufnahme. Package Builder analysiert die Unterschiede und kann so alle Änderungen ermitteln, die auf dem Computer erfolgt sind. Anschließend wird ein Konfigurationsskript für die Paketverteilung erstellt. Diese Datei besitzt die Dateinamenerweiterung .CFG und wird im Ordner c:\Program Files\Intel\Package Builder\Working des Paketerstellungscomputers abgelegt.

Diese .CFG-Skriptdatei enthält Änderungen an der Registrierung, am Dateisystem, am Desktop und an anderen Systemressourcen. Für entfernte Elemente wird jedoch keine Steuerungsdatei erstellt, d. h. eine Deinstallationsoption müssen Sie manuell hinzufügen, entweder wenn Sie das Skript bearbeiten oder seine Verteilung planen.

Sobald diese Änderungen gespeichert sind, zeigt der Package Builder-Assistent die Option zum Kompilieren der .CFG-Datei in eine ausführbare Datei an. Sie haben jedoch auch die Möglichkeit, die Datei in Package Builder zu öffnen, um weitere Änderungen vorzunehmen. Klicken Sie auf "Bearbeiten", um die neue .CFG-Datei in Package Builder zu öffnen, und nehmen Sie die Änderungen vor. Wenn Sie mit der Installation einverstanden sind, klicken Sie auf "Erstellen", um das Paket zu erstellen.

Sobald der Vorgang abgeschlossen ist, wird eine Seite mit dem Hinweis angezeigt, dass das Paket erstellt und im Standardverzeichnis des Paketerstellungscomputers gespeichert wurde.

4. Wiederherstellen des Paketerstellungscomputers

Wenn Sie mit der Paketerstellung fertig sind, sollten Sie den Paketerstellungscomputer auf den Status vor der Installation zurücksetzen. Damit wird sichergestellt, dass der Computer "sauber" ist, bevor das nächste Paket erstellt wird. ESWD enthält keinen Prozess zum Zurücksetzen des Computers. Daher sollten Sie ein Programm zur Verarbeitung von Computerabbildern verwenden, wie das LANDesk Abbildverarbeitungstool, das Teil der Betriebssystem-Verteilung ist, Symantec Ghost* o. ä., um das Betriebssystem des Clients wiederherzustellen.

Wenn Sie ein Dienstprogramm wie Ghost zum Wiederherstellen des Paketerstellungscomputers verwenden, wird auch die .CFG-Datei gelöscht, mit der das Paket erstellt wurde. Wenn diese Dateien weiterhin zur Verfügung stehen sollen, um sie in zukünftigen Paketen zu verwenden oder zu einem späteren Zeitpunkt zu bearbeiten, können Sie sie auf einer Netzwerkfreigabe speichern. Geben Sie einfach ein Netzwerkverzeichnis auf der Seite "Optionen" des Assistenten an, um diese Dateien zu behalten.

Jeder neue Systemscan wird standardmäßig in einem neuen Arbeitsverzeichnis gespeichert. Sie können denselben Ordner jedoch erneut verwenden, wenn Sie den alten Systemscan überschreiben möchten. Manche Benutzer speichern Softwareabbilder mehrerer Betriebssysteme auf einem einzigen Paketerstellungscomputer. Diese Lösung bietet optimale Flexibilität bei der Erstellung von Softwarepaketen, ohne dass mehrere Computer speziell für die Softwarepaketerstellung angegeben werden müssen.

Ausführen des Package Builder-Assistenten

Wie bereits beschrieben wird ein Softwareverteilungspaket in zwei Schritten erstellt. Im ersten Schritt wird ein Installationsskript (.CFG-Datei) im Arbeitsverzeichnis von Package Builder erstellt. Das Skript enthält alle Clientanweisungen für die Installation der Software. Im zweiten Schritt wird das Softwareverteilungspaket erstellt. Das Paket enthält die Anweisungen und die Dateien.

Neben den Paketen, die mit dem Package Builder-Assistenten erstellt werden, unterstützt der ESWD-Agent geplante oder richtlinienbasierte Bereitstellungen für drei andere Pakettypen:

- Einzel- und Multidatei-MSI-Pakete
- Legacypakete aus vorherigen Versionen von LANDesk Management Suite
- Selbstextrahierende ausführbare Dateien

Wenn Sie diese Pakettypen verwenden, können Sie diesen Task überspringen und mit "Einrichten des Übermittlungsservers" weiter unten in diesem Kapitel fortfahren.

So führen Sie den Package Builder-Assistenten aus

1. Klicken Sie auf dem Paketerstellungscomputer auf **Start** | **Programme** | **LANDesk Management** | **Package Builder-Assistent**.
2. Klicken Sie auf **Scanoptionen**, um den Scanprozess zu konfigurieren. Auf dieser Seite können Sie auswählen, in welchen Verzeichnissen Änderungen vom Assistenten überwacht werden und ob der Assistent eine Sicherung erstellt, damit nach dem Erstellen des Pakets der aktuelle Status des Clients wiederhergestellt werden kann. Wenn Sie alle Änderungen in das Formular eingegeben haben, klicken Sie auf **OK**.

Mindestens ein logisches oder physisches Laufwerk muss überwacht werden
Der Package Builder-Assistent muss mindestens ein logisches oder physisches Laufwerk überwachen, um Änderungen an Systeminformationen verfolgen zu können. Wenn Sie das angegebene Standardlaufwerk auf der Seite "Scanoptionen" löschen und keine Laufwerke für die Überwachung ausgewählt sind, wird der Assistent beendet.

---

3. Klicken Sie auf **Buildoptionen**, um benutzerspezifische Einstellungen für Windows NT- und Windows 2000/2003/XP-Systeme zu konfigurieren. Sie können auswählen, ob diese Einstellungen nur für den angemeldeten Benutzer (bzw. den Standardbenutzer, falls derzeit kein Benutzer angemeldet ist) oder für alle Benutzer gelten sollen. Diese benutzerspezifischen Einstellungen umfassen Elemente des Startmenüs, Kurzbefehle und Registrierungseinstellungen für den Schlüssel HKEY_CURRENT_USER. Um zurückzukehren, klicken Sie auf **OK**.
4. Klicken Sie auf **Weiter**. Der Assistent überprüft das System.
5. Wählen Sie die Methode für die Installation der Anwendung aus.

   - Wenn das Installationsprogramm lokal verfügbar ist (z. B. als SETUP.EXE-Programm), klicken Sie auf **Durchsuchen**, um nach dem Installationsprogramm zu suchen. Wählen Sie es aus und klicken Sie auf **Überwachen**.
   - Wenn das Installationsprogramm auf einer Autorun-CD gespeichert ist, klicken Sie auf **Weiter**, und legen Sie die CD ein.
   - Um andere Änderungen für ein Softwareverteilungspaket vorzunehmen (beispielsweise Dateien kopieren oder Desktopverknüpfungen erstellen), klicken Sie auf **Weiter**, und führen Sie das entsprechende Dienstprogramm aus.
6. Folgen Sie den Eingabeaufforderungen, um die Software zu installieren.
7. Wenn die Installation abgeschlossen ist, geben Sie einen Namen für das Paket ein. Sie sollten einen Namen verwenden, der sowohl die Software als auch das Betriebssystem wiedergibt, z. B. WinZip_Win2K für ein Paket, das WinZip auf einem Client mit Windows 2000/2003 installiert.
8. Klicken Sie auf **Vergleichen**.
9. Wenn die .CFG-Datei erstellt wurde, klicken Sie auf **OK** und anschließend auf **Erstellen**.
   Hinweis: Die .CFG-Datei kann angepasst und dann in ein Paket eingefügt werden. Weitere Informationen finden Sie im "Skript-Handbuch für .CFG-Dateien" in Anhang C.
10. Wenn die Erstellung abgeschlossen ist, legt der Assistent das Paket im Ordner Onefile des Package Builder-Arbeitsverzeichnisses ab. Für das Paket wird der von Ihnen ausgewählte Name verwendet und die Erweiterung .EXE angehängt. Klicken Sie auf **Fertigstellen**. Sie können dieses Paket manuell testen, indem Sie auf die .EXE-Datei klicken.

Anschließend müssen Sie den Übermittlungsserver einrichten und dieses Paket darauf kopieren.

Einrichten des Übermittlungsservers

Der Übermittlungsserver ist der Server, auf dem Softwareverteilungspakete gespeichert werden. Dabei kann es sich entweder um einen Webserver oder einen Windows NT/2000/2003-Server handeln.

Übermittlungsserver	Anforderungen
Webserver	Microsoft Internet Information Server 5.0 oder höher, ausgeführt unter Windows NT oder Windows 2000/2003
Netzwerkserver	Windows NT 4.0 oder Windows 2000/2003

So konfigurieren Sie einen Webserver für die Softwareverteilung

In den folgenden Schritten wird beschrieben, wie ein virtuelles Verzeichnis auf einem Webserver erstellt und für Suchvorgänge aktiviert wird. Im Allgemeinen gilt, dass sich virtuelle Verzeichnisse lesen und durchsuchen lassen müssen. Die Berechtigung zum Ausführen darf nicht aktiviert sein, weil die Freigabe sonst nicht korrekt funktioniert. Außerdem sollten Sie Schreibberechtigungen deaktivieren, damit Clients den Verzeichnisinhalt nicht ändern können.

1. Erstellen Sie ein Verzeichnis auf dem Webserver, in dem die Softwareverteilungspakete gespeichert werden sollen. Im Normalfall wird dafür auf einem IIS-Webserver ein Unterverzeichnis des Verzeichnisses c:\inetpub\wwwroot verwendet.
2. Kopieren Sie die Pakete in dieses Verzeichnis.
3. Doppelklicken Sie in der Systemsteuerung auf **Verwaltung** und anschließend auf **Internetdienste-Manager**.
4. Doppelklicken Sie im rechten Bereich auf das Symbol mit dem Namen des Clients, und klicken Sie auf **Standardwebsite**.
5. Klicken Sie im rechten Bereich mit der rechten Maustaste auf eine freie Stelle, wählen Sie **Neu**, und klicken Sie auf **Virtuelles Verzeichnis**.
6. Klicken Sie im Assistenten auf **Weiter**, und geben Sie einen Alias für das Verzeichnis ein. Klicken Sie auf **Weiter**.
7. Geben Sie den Pfad ein, oder wechseln Sie zum gewünschten Pfad, und klicken Sie auf **Weiter**.
8. Aktivieren Sie im Dialogfeld "Zugriffsberechtigungen" die Optionen **Skript ausführen** und **Durchsuchen**. So können Sie Pakete beim Erstellen des Softwareverteilungsskripts durchsuchen. Klicken Sie auf **Weiter** und auf **Fertig stellen**.
9. Um **Port 80** auf dem Webserver zu aktivieren, klicken Sie im linken Bereich mit der rechten Maustaste auf **Standardwebsite**.
10. Klicken Sie auf **Eigenschaften**. Im Dialogfeld "Identifikation der Webseite" muss im Feld "TCP-Port" der Wert 80 angezeigt werden. Andernfalls müssen Sie auf **Erweitert** klicken, um den Port hinzuzufügen.

11. Stellen Sie sicher, dass die Website verfügbar ist, indem Sie einen Browser öffnen und den URL des Webservers sowie ein virtuelles Verzeichnis eingeben. Wenn der Webserver "Test" heißt und der Name des virtuellen Verzeichnisses "Pakete" lautet, geben Sie folgenden URL ein:

    ```
    http://Test/Pakete
    ```

    Eine Liste der Pakete, die in dieses Verzeichnis kopiert wurden, wird angezeigt.

Sofern der Speicherplatz der Festplatte dies zulässt, können Sie Pakete in beliebiger Größe und Anzahl in diesem Verzeichnis speichern. Unterverzeichnisse können so erstellt werden, dass Pakete logisch gruppiert werden können. Für jedes erstellte Unterverzeichnis müssen die oben beschriebenen Zugriffsberechtigungen festgelegt werden.

Sobald Sie die Pakete auf eine Paketfreigabe eines Webservers kopiert haben, werden sie bereitgestellt und können auf die Zielclients kopiert werden. Wenn das Paket an der Reihe ist, wird sein URL oder UNC-Pfad als Befehlszeilenparameter an SDCLIENT.EXE (den Clientagent) übergeben. SDCLIENT.EXE verwaltet die Dateiübertragung, startet die Installation und erstellt Statusberichte. Für die Dateiübertragung wird zwar das HTTP-Protokoll verwendet, der Statusbericht wird jedoch über CBA zurückgegeben.

Der Webserver kommuniziert mit dem Client, um sicherzustellen, dass das Paket richtig kopiert wird. Wenn die Paketübertragung beim Download unterbrochen wird, kann der Webserver den Download mithilfe des HTTP-Protokolls an der Stelle fortsetzen, an der er unterbrochen wurde. Der Webserver überprüft jedoch nicht, ob das Paket richtig installiert wurde. Dieser Verkehr basiert auf UDP, der Status wird mithilfe von CBA an den Core Server zurückgegeben.

So konfigurieren Sie einen Netzwerkserver für die Softwareverteilung

Clients, die keinen Browser besitzen, müssen Verteilungspakete über einen UNC-Pfad auf einem Windows NT/2000/2003-Netzwerkserver erhalten. Dazu kann dasselbe Verzeichnis verwendet werden, das auch auf dem Webserver eingerichtet wurde. Damit Verteilungen über den UNC-Pfad richtig ausgeführt werden, müssen Sie einen NULL-Sitzungsfreigabeordner auf dem Netzwerkserver aktivieren. Verwenden Sie das Dienstprogramm SYSSHRS.EXE, um einen NULL-Sitzungsfreigabeordner zu erstellen.

1. Um einen freigegebenen Ordner auf dem Netzwerkserver einzurichten, klicken Sie mit der rechten Maustaste auf den Ordner, der freigegeben werden soll, und klicken Sie auf **Freigabe**.
2. Klicken Sie auf **Diesen Ordner freigeben** und anschließend auf **Berechtigungen**.
3. Fügen Sie die Gruppen **Jeder** und **Gast** hinzu. Weisen Sie ihnen jedoch nur Leseberechtigung zu. Übernehmen Sie die Änderungen.
4. Klicken Sie auf dem Netzwerkserver auf **Start | Ausführen**, und wechseln Sie zum Verzeichnis LDMAIN\Utilities auf dem Core Server.
5. Führen Sie das Dienstprogramm **SYSSHRS.EXE** aus.
   Hinweis: In diesem Dienstprogramm wird zwar angegeben, dass es für Windows NT-Clients verwendet werden kann, es funktioniert jedoch auch auf Windows 2000/2003-Clients.

6. Überprüfen Sie den freigegebenen Ordner, den Sie eingerichtet haben, und klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.
7. Kopieren Sie die Softwareverteilungspakete in dieses Verzeichnis auf dem Netzwerkserver.

Sofern der Speicherplatz der Festplatte dies zulässt, können Sie Pakete in beliebiger Größe und Anzahl auf dem Netzwerkserver speichern.

Weitere Informationen zum Dienstprogramm SYSSHRS.EXE erhalten Sie, indem Sie das Paket SHARES.EXE von der Website http://www.landesk.com/support/downloads/detail.php?rid=52 herunterladen und die Dokumentation extrahieren.

Konfigurieren eines Windows 2003-Webservers für die Softwareverteilung

Windows 2003 Server behandelt virtuelle Verzeichnisse anders als Windows 2000. Wenn Sie auf einem Windows 2003-Server ein Verzeichnis auswählen und es über das Kontextmenü als Webfreigabe festlegen, registriert sich das Verzeichnis in IIS 6 selbst als Webanwendung statt als virtuelles Verzeichnis. Problematisch an der Registrierung als Webanwendung ist hierbei, dass der Webserver bei der Auswahl einer ausführbaren Datei versucht, die Datei als Webanwendung auszuführen statt sie zum Benutzer herunterzuladen. Die Lösung besteht darin, das freigegebene Verzeichnis im IIS von einer Webanwendung in ein virtuelles Verzeichnis zu ändern und die Berechtigungen zum Ausführen zu deaktivieren..

Wenn Dateien auf einem Windows 2003-Server bereitgestellt werden, können Dateien, die keinen registrierten MIME-Dateityp besitzen, nur dann per Multicast verteilt werden, wenn Sie folgende Schritte ausführen.

So registrieren Sie MIME-Dateitypen

1. Starten Sie den Internetinformationsdienste-Manager (IIS).
2. Erweitern Sie den lokalen Computer in der Strukturansicht.
3. Klicken Sie auf **Websites > Standardwebsite**.
4. Klicken Sie im Kontextmenü der Webfreigabe, die das Paket enthält, auf **Eigenschaften**.
5. Klicken Sie auf das Register **HTTP-Header**.
6. Klicken Sie auf **MIME-Typen**.
7. Klicken Sie auf **Neu**.
8. Geben Sie im Feld **Erweiterung** einen Stern (*) ein.
9. Geben Sie im Feld **MIME-Typ** einen beliebigen Namen an.
10. Klicken Sie zweimal auf **OK** und übernehmen Sie die Änderungen.

Konfigurieren von Clients für den Empfang von Paketen

Auf den Clients, welche die Softwareverteilungspakete empfangen, müssen folgende LANDesk-Agenten installiert sein.

- Common Base Agent (CBA)
- Bandbreitenerkennungsagent
- Enhanced Software Distribution-Agent

Falls Sie Targeted Multicast verwenden möchten, muss der Targeted Multicast-Agent ebenfalls auf den Clients installiert sein.

Um den Agenten mehreren Clients bereitzustellen, empfiehlt sich die Verwendung eines automatisierten Prozesses. Eine Methode wäre beispielsweise, die Befehle in das Anmeldeskript einzufügen, damit sie ausgeführt werden, sobald sich Clients beim Netzwerk anmelden. Weitere Informationen finden Sie im *Installations- und Verteilungshandbuch*.

Gehen Sie entsprechend den folgenden Anweisungen vor, um einen Client zu konfigurieren.

So installieren Sie die Clientsoftware

1. Stellen Sie vom Client aus eine Verbindung zum LDLogon-Verzeichnis auf dem Core Server her.
2. Führen Sie **WSCFG32.EXE** aus, und installieren Sie die folgenden Agenten (sofern sie noch nicht installiert sind):
    - Common Base Agent
    - Bandbreitenerkennung
    - Enhanced Software Distribution
    - Targeted Multicast

Verteilen eines Pakets

In diesen Anweisungen wird beschrieben, wie ein Softwareverteilungsskript erstellt wird. Damit das Skript richtig ausgeführt wird, muss das Softwareverteilungspaket auf einem Netzwerk- oder Webserver bereitstehen. Auf den Clients muss der ESWD-Agent installiert sein.

So erstellen Sie ein Paketverteilungsskript

1. Erstellen Sie das Paket, das Sie verteilen möchten.
2. Klicken Sie auf **Extras | Skripte verwalten**.
3. Klicken Sie auf die Schaltfläche **Neues Verteilungsskript**.
4. Wählen Sie das Softwareverteilungspaket aus, indem Sie auf **Webfreigabe** oder **Dateisystemfreigabe** klicken:
   - Bei einem Webserver geben Sie den URL für das Webserververzeichnis in das Feld ein und drücken die **Eingabetaste**. Wählen Sie das Paket aus. (Das Durchsuchen des Verzeichnisses muss auf dem Webserver aktiviert werden. Weitere Informationen finden Sie unter "Einrichten des Übermittlungsservers" weiter oben in diesem Kapitel.)
   - Bei einem Netzwerkserver geben Sie den Pfad zum Paket ein, oder klicken Sie auf **Durchsuchen**, und wechseln Sie in das Verzeichnis des Pakets. (UNC-Pfade müssen auf dem Netzwerkserver aktiviert werden. Weitere Informationen finden Sie unter "Einrichten des Übermittlungsservers" weiter oben in diesem Kapitel.)
   - Klicken Sie nach dem Auswählen des Pakets auf "Weiter".
5. Klicken Sie auf der Seite "Skript erstellen" auf **Installieren** oder **Deinstallieren**, je nachdem, welchen Pakettyp Sie verteilen.
6. Geben Sie einen **Skriptnamen** ein.
7. Aktivieren Sie die Option **Dieses Paket mit Multicast verteilen**, wenn Sie Targeted Multicast verwenden. In diesem Fall können Sie auch die Option **Nur eine einzige Datei mit Multicast kopieren** aktivieren. Verwenden Sie diese Option, wenn Sie nur eine einzige Datei verteilen möchten. Klicken Sie auf **Weiter**.
8. Beenden Sie den Assistenten. Klicken Sie auf **Hilfe**, um weitere Informationen zu den einzelnen Seiten abzurufen. Sobald Sie fertig sind, wird das neue Skript im Zweig "Alle anderen Skripts" des Baumes "Skripte verwalten" angezeigt.

So planen Sie die Verteilung eines Skripts

1. Klicken Sie im Fenster **Skripte verwalten** auf **Skripte > Eigene Skripte** oder **Alle anderen Skripte** und auf das Skript, das Sie verteilen möchten.
2. Klicken Sie auf die Schaltfläche **Task erstellen**. Anschließend wird das Fenster **Geplante Tasks** mit dem von Ihnen ausgewählten Skript angezeigt.
3. Suchen Sie in der Netzwerkansicht nach den Clients, die aktualisiert werden sollen, und verschieben Sie ihre Symbole mittels Ziehen-und-Ablegen in den rechten Bereich des Fensters **Geplante Tasks**.
4. Klicken Sie im Fenster **Geplante Tasks** auf die Schaltfläche **Startzeit festlegen**, um das Dialogfeld **Task planen** anzuzeigen.

5. Legen Sie die gewünschten Zeitoptionen fest. Klicken Sie auf **Jetzt starten** und auf **OK**, wenn die Aktualisierung des Clients so bald wie möglich erfolgen soll.

In diesem Dialogfeld wird angezeigt, ob der Auftrag abgeschlossen ist. Sollte eine Installation fehlschlagen, werden hier wichtige Fehlercodes angezeigt. Diese Fehlercodes können Ihnen helfen, Probleme bei der Paketverteilung zu beheben. Sobald im Dialogfeld angezeigt wird, dass der Auftrag abgeschlossen ist, ist das Paket bereitgestellt. Weitere Informationen zu den Fehlercodes für Clients finden Sie unter "Bedeutung der Enhanced Software Distribution-Fehlercodes" in Anhang C.

Sie können mithilfe von Abfragen eine Liste der Clients erstellen, an die Pakete verteilt werden sollen. Weitere Informationen zur Erstellung von Abfragen finden Sie in Kapitel 3 "Verwenden von Abfragen".

Checkpunkt-Neustarts auf Byte-Ebene und dynamische Bandbreitendrosselung

Management Suite 8 und neuere Versionen unterstützen bei der Verteilung Checkpunkt-Neustarts auf Byte-Ebene und dynamische Bandbreitendrosselung. Checkpoint-Neustarts können bei Verteilungsaufträgen ausgeführt werden, die von ESWD zuerst in das Cacheverzeichnis des Clients (standardmäßig C:\LDCLIENT\SDMCACHE) kopiert werden. Normalerweise werden ESWD- und MSI-Pakete erst während der Installation des Pakets in den Clientcache kopiert, weil bei diesen Pakettypen nur die benötigten Paketteile heruntergeladen werden, wodurch die Downloadmenge möglichst klein gehalten wird. Alle anderen Pakettypen und Dateien werden zuerst in den Clientcache kopiert, und Checkpoint-Neustarts ermöglichen es, dass unterbrochene Verteilungsvorgänge an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden.

Dynamische Bandbreitendrosselung legt fest, dass der von einem Client erzeugte Netzwerkverkehr Vorrang vor dem durch die Verteilung bedingten Verkehr hat. Diese Option erzwingt zudem, dass die gesamte Datei in den Cache des Clients heruntergeladen wird. Damit wird gleichzeitig die Option für Checkpoint-Neustarts auf Byte-Ebene aktiviert, sodass Downloadvorgänge im Fall einer Unterbrechung an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden. Wenn Sie diese Option auswählen und die Prozentangabe für **Minimal verfügbare Bandbreite** auf 0 belassen, wird die Verteilung auf etwa ein Paket pro Sekunde gedrosselt, sobald der Client Netzwerkverkehr initiiert, und bleibt auf diesem Niveau, bis der Netzwerkverkehr endet. Durch die Erhöhung der minimal verfügbaren Bandbreite wird etwa die von Ihnen angegebene Menge an Clientbandbreite für die Verteilung reserviert, wenn zur Verteilung Netzwerkbandbreite erforderlich ist und Anwendungen auf dem Client um Bandbreite konkurrieren.

Wenn Sie ein ESWD- oder MSI-Paket erneut installieren oder reparieren, sollten Sie die Option für die dynamische Bandbreitendrosselung nicht verwenden, weil bei diesen Pakettypen normalerweise nur die benötigten Dateien heruntergeladen werden. In diesem Fall würde durch den Einsatz der dynamischen Bandbreitendrosselung auch dann ein Download des gesamten Pakets erzwungen, wenn nur ein kleiner Teil des Pakets zur Reparatur benötigt wird.

Die dynamische Bandbreitendrosselung ist auf Windows 95/98-Computern nicht verfügbar.

Arbeiten mit Mac OS X-Verteilungsskripten und -paketen

Sie können ein Skript erstellen, um mit dem normalen Verteilungsverfahren oder mit Targeted Multicast Pakete mit ausführbaren Einzeldateien auf Macintosh OS X-Clients zu verteilen. Jedes Skript verteilt nur eine Datei und der Client versucht, die Datei auszuführen, sobald der Client sie erhalten hat. Sie müssen den Mac OS X-Client von Management Suite auf den Zielcomputern installieren, bevor Sie auf den Computern Dateien verteilen können.

Macintosh OS X-Verteilungsskripts werden wie Windows-Verteilungsskripts behandelt.. Die Skripts werden als Textdateien gespeichert und Sie können sie nach ihrer Erstellung bei Bedarf manuell bearbeiten.. Sie können Mac OS X-Verteilungsskripts im Fenster "Geplante Tasks" planen und Mac OS X-Clients als Verteilungsziele in das Fenster "Geplante Tasks" ziehen.

So erstellen Sie ein Mac OS X-Softwareverteilungsskript

1. Erstellen Sie das Paket, das Sie verteilen möchten.
2. Klicken Sie auf **Extras | Skripte verwalten**.
3. Klicken Sie auf die Schaltfläche **Neues Macintosh Distribution Script**.
4. Wählen Sie das erstellte Softwareverteilungspaket aus.
   - Bei einem Webserver geben Sie den URL für das Webserververzeichnis in das Feld **URL** ein und drücken die **Eingabetaste**. Wählen Sie das Paket aus. (Das Durchsuchen des Verzeichnisses muss auf dem Webserver aktiviert werden. Weitere Informationen finden Sie unter "Einrichten des Übermittlungsservers" weiter oben in diesem Kapitel.)
   - Bei einem Netzwerkserver klicken Sie auf **Durchsuchen** und wechseln in das Verzeichnis des Pakets. (UNC-Pfade müssen auf dem Netzwerkserver aktiviert werden. Weitere Informationen finden Sie unter "Einrichten des Übermittlungsservers" weiter oben in diesem Kapitel.)
5. Wählen Sie im Assistenten für die Paketbereitstellung die Option **Paket auf Macintosh-Clients verteilen**. Klicken Sie auf **Weiter**.
6. Geben Sie den Skriptnamen auf der Seite "Skript erstellen" ein. Klicken Sie auf **Weiter**.
7. Beenden Sie den Assistenten. Klicken Sie auf **Hilfe**, um weitere Informationen zu den einzelnen Seiten abzurufen. Sobald Sie fertig sind, wird das neue Skript im Zweig "Alle anderen Skripts" des Baumes "Skripte verwalten" angezeigt.

Macintosh-Skripts bearbeiten

Macintosh-Skriptbefehle können entweder Download- oder Shellbefehle sein. Downloadbefehle beginnen mit "http://" oder mit "ftp://". Per Definition ist es ein Shellbefehl, wenn es sich nicht um einen Downloadbefehl handelt. Allen Macintosh-Skriptbefehlen muss ldkahuna vorangestellt werden. Beispiele:

```
REMEXEC0=ldkahuna "http://..."
```

Damit Macintosh-Skriptbefehle korrekt ausgeführt werden, können Sie auch Folgendes tun:

- Der Befehl, der dem Eintrag ldkahuna folgt, sollte in Anführungszeichen eingeschlossen sein.
- In URLs sollten Escapesequenzen verwendet werden ("%20" für Leerzeichen usw.).
- In Befehlen sollten ebenfalls Escapesequenzen verwendet werden (für ein Leerzeichen sollte die Sequenz "umgekehrter Schrägstrich plus Leerzeichen" angegeben werden usw.).
- Argumente müssen in einfache Anführungszeichen eingeschlossen werden.

Es kann jede Datei heruntergeladen werden, Verzeichnisse werden mit Management Suite jedoch nicht heruntergeladen. Installationspakete (.PKG) können Verzeichnisse enthalten. Sie müssen komprimiert werden. Wenn die heruntergeladene Datei die Erweiterung .SIT, .ZIP, .TAR, .GZ, .SEA oder .HQX besitzt, entkomprimiert Management Suite die Datei vor der Rückgabe. (Benutzer müssen sich vergewissern, dass in Stuffit Expander* die Option zum Suchen nach neuen Versionen deaktiviert ist. Andernfalls wird die Skriptausführung u. U. durch ein Dialogfeld unterbrochen.)

Der OS X-Agent führt Dateien nicht automatisch aus. Mit dem Shellbefehl "open" können Benutzer Dateien oder Anwendungen öffnen, mit dem Shellbefehl "installer" können sie .PKG-Dateien installieren.

Die Downloaddatei kann auch ein in Perl geschriebenes Shellskript sein usw. Nachdem die Datei auf die Clients heruntergeladen wurde, können Sie die Datei mit einem Shellbefehl ausführen. Shellbefehle werden als Root ausgeführt.

Dateien werden in das Verzeichnis /Library/Application Support/LANDesk/sdcache/ heruntergeladen. Diese Information benötigen Sie für die Shellbefehle.

Verteilen von Dateien mit einem Dateiübertragungsskript

Wenn Sie nur Dateien auf Clients kopieren möchten, können Sie ein Dateiübertragungsskript verwenden. Sie können jeden Dateityp, einschließlich Textdateien, in ein angegebenes Verzeichnis auf dem Client übertragen. Dateiübertragungsskripts unterstützen Targeted Multicast.

So verteilen Sie Dateien

1. Klicken Sie auf **Extras | Skripte verwalten**.
2. Klicken Sie im Kontextmenü **Alle anderen Skripts** auf **Dateibereitstellungsskript erstellen**.
3. Geben Sie einen **Skriptnamen** und ein **Zielverzeichnis** ein. Klicken Sie auf **Weiter**.
4. Geben Sie die gewünschten Multicast-Domänenoptionen an. Klicken Sie auf "Weiter".
5. Wählen Sie die bereitzustellenden Dateien aus, indem Sie **Webpfad** oder **Dateifreigabepad** auswählen. Geben Sie den Pfad ein, und fügen Sie der Liste die gewünschten Dateien hinzu. Klicken Sie auf **Weiter**.
6. Lesen Sie die Zusammenfassung auf der Seite **Fertig**, und klicken Sie auf **Fertigstellen**.

Informationen zur Seite "Dateibereitstellungsskript erstellen"

Verwenden Sie den Assistenten "Dateibereitstellungsskript" (Fenster "Skripte verwalten" > Kontextmenü "Alle anderen Skripts" > Dateibereitstellungsskript erstellen), um einzelne Dateien eines beliebigen Typs in einem angegebenen Clientverzeichnis bereitzustellen.

- **Skriptname:** Geben Sie einen beschreibenden Namen für das Skript ein, das Sie erstellen.
- **Zielverzeichnis:** Geben Sie das Clientverzeichnis ein, in dem die Dateien abgelegt werden sollen.

Deinstallieren von Softwareverteilungspaketen

ESWD bietet folgende Methoden zum Deinstallieren von Paketen, die erstellt und an Clients verteilt wurden:

- Deinstallationsbefehl in Package Builder
- Deinstallationsoption in der Konsole
- Deinstallationspaket im Package Builder-Assistenten

Deinstallationsbefehl in Package Builder

Sie können den Deinstallationsbefehl in Package Builder für alle Pakete aktivieren, die an Clients verteilt werden. Mit diesem Befehl erstellen die Pakete bei ihrer Installation eine eigene ausführbare Deinstallationsdatei im Standardverzeichnis der Anwendung auf dem Client. Sie können dann ein Skript erstellen, um diese Deinstallationsdatei auf dem Client zu aktivieren und das Paket zu entfernen.

Vorteile dieser Methode:

- Die Deinstallation wird vom Skript ausgelöst, und die installierten Dateien werden komplett entfernt.
- Alle Dateizähler werden bei der Deinstallation richtig angepasst. Das bedeutet, dass .DLL-Dateien, die auch von anderen Programmen auf dem Client genutzt werden, nicht entfernt werden.

Nachteile dieser Methode:

- Der Deinstallationsbefehl muss im ursprünglich erstellten Paket enthalten sein.
- Der Benutzer wird aufgefordert, die Anwendung zu entfernen. Wenn der Benutzer mit "Nein" antwortet, wird das Paket nicht deinstalliert. Diese Eingabeaufforderung kann nicht unterdrückt werden.
- Da die Deinstallationsdatei auf dem Client gespeichert wird, kann ein Benutzer das Softwarepaket ohne Ihr Wissen deinstallieren. Die Deinstallationsdatei wird in der Systemsteuerung unter "Software" angezeigt.
- Sie müssen den richtigen Pfad kennen, um auf die Datei zugreifen zu können.

Das folgende Beispiel zeigt die Syntax eines Skripts, mit dem die Deinstallationsdatei WinZip vom Client entfernt:

```
[MACHINES]
REMEXEC0="C:\Program Files\WinZip\UninstallINSTALL.EXE"
```

REMEXECO ist der Fernausführungsbefehl

"C:\Program Files\WinZip\Uninstall INSTALL.EXE" ist der vollständige Pfad zur Deinstallationsdatei. Wenn Pfadnamen Leerzeichen enthalten, müssen Anführungszeichen verwendet werden. Der Standardname dieser Datei lautet "Uninstall" + der Name des Softwareverteilungspakets.

Sobald Sie ein Skript für ein Deinstallationspaket erstellt haben, planen Sie die Verteilung an die Benutzer, um das Paket zu deinstallieren.

Deinstallationsoption in der Konsole

Sie können die Werkzeuge in der Konsole zum Deinstallieren der verteilten Pakete verwenden. Klicken Sie in der Konsole auf **Extras | Skripte verwalten** und dann auf die Schaltfläche **Neues Verteilungsskript**. Wählen Sie das .EXE-Paket aus, mit dem die Software installiert wurde. Klicken Sie im Fenster "Skript erstellen" auf **Deinstallieren**. Dadurch wird ein "Alle entfernen"-Flag im Paket gesetzt, und alle im Installationsskript installierten Elemente werden entfernt.

Vorteile dieser Methode:

- Die ausführbare Deinstallationsdatei befindet sich nicht auf dem Client.
- Mit dieser ausführbaren Datei können Softwareverteilungspakete deinstalliert werden, die nicht mit dem Deinstallationsbefehl erstellt wurden.

Deinstallationspaket im Package Builder-Assistenten

Wenn Sie mit den bereits beschriebenen Methoden nicht die gewünschten Ergebnisse erzielen, können Sie auf eine andere Option zurückgreifen. Mit dem Package Builder-Assistenten können Sie ein Paket des Deinstallationsprozesses auf dem Paketerstellungscomputer erstellen und dieses dann an die Clients verteilen.

Diese Methode wird nicht empfohlen
Wenn die Anwendung, die deinstalliert werden soll, .DLL-Dateien verwendet, die auch von anderen Anwendungen genutzt werden, können mit dieser Methode .DLL-Dateien entfernt werden, die von anderen Anwendungen benötigt werden.

So erstellen Sie ein Deinstallationspaket

1. Starten Sie den **Package Builder-Assistenten** auf dem Paketerstellungscomputer. Die Anwendung, die von den Clients entfernt werden soll, sollte bereits mit denselben Standardeinstellungen wie auf den Clients installiert sein.
2. Klicken Sie auf **Weiter**, um die "Vorher"-Statusaufnahme zu starten. Klicken Sie anschließend erneut auf **Weiter**. *Klicken Sie nicht auf die Schaltfläche "Durchsuchen".* Wenn Sie auf "Durchsuchen" klicken, wird die Installation für eine andere Anwendung gestartet. In diesem Fall soll jedoch eine Anwendung deinstalliert werden.
3. Sobald die "Vorher"-Statusaufnahme abgeschlossen ist, drücken Sie **Alt+Tab**, um in eine andere Anwendung zu wechseln. *Klicken Sie nicht auf die Schaltfläche "Durchsuchen".*
4. Klicken Sie auf **Start** | **Einstellungen** | **Systemsteuerung**, um die Systemsteuerung zu öffnen.
5. Doppelklicken Sie auf das Symbol **Software**, um das Dialogfeld "Eigenschaften" zu öffnen. Klicken Sie auf dem Register **Installieren/Deinstallieren** auf die Anwendung, die entfernt werden soll, und anschließend auf **Hinzufügen/Entfernen**.

   Wenn die Anwendung ein eigenes Deinstallationsprogramm besitzt, sollten Sie es nun ausführen.

6. Sobald die Anwendung deinstalliert ist, drücken Sie **Alt+Tab**, um zum Package Builder-Assistenten zurückzukehren.
7. Geben Sie den **Namen** für dieses Deinstallationspaket ein, und klicken Sie auf **Vergleichen**, um die "Nachher"-Statusaufnahme zu starten. Sobald sie abgeschlossen ist, wird das Dialogfeld "Gratulation" angezeigt. Klicken Sie auf **OK**, um es zu schließen.
8. Wenn das Dialogfeld "Bereit zum Erstellen" angezeigt wird, klicken Sie auf **Erstellen** und anschließend auf **Fertigstellen**, um die Paketerstellung abzuschließen.

Sie können dieses Paket an die Clients verteilen.

Kapitel 7: Verwenden der Webkonsole

Info zur Webkonsole

Die Webkonsole umfasst eine Auswahl der Management Suite-Funktionen und bietet die Vorteile eines Webbrowsers. Die Management Suite-Konsole ist zwar Ihre wichtigste Ressource beim Verwalten der Computer, die Webkonsole ist jedoch hilfreich, wenn die Verwaltungskonsole nicht verfügbar ist. Weitere Informationen finden Sie unter "Stufe 6: Installieren der Webkonsole" im *Installations- und Verteilungshandbuch.*

Sobald die Webkonsole eingerichtet ist, können Sie über einen Browser von den meisten Computern im Netzwerk darauf zugreifen. Verwenden Sie die Webkonsole für folgende Zwecke:

- Fernsteuern von Computern
- Ausführen von Inventarabfragen
- Anzeigen von Berichten über Computerinventar
- Planen und Verteilen von Softwarepaketen auf Computern
- Anzeigen einzelner Inventarübersichten für Computer
- Fernaktivierung von ausgeschalteten Computern

Sobald Sie die Webkonsole installiert und ein Konto eingerichtet haben, können Sie die Webkonsole auf jedem Computer aufrufen, auf dem Internet Explorer 5.5 oder höher ausgeführt wird.

So führen Sie die Webkonsole aus

1. Öffnen Sie einen Webbrowser auf einem Netzwerkcomputer.
2. Geben Sie im Feld "Adresse" am oberen Rand des Browsers den URL ein, der Sie mit der Site der Webkonsolenseiten verbindet, in der Regel http://webservername/remote.
3. Wird ein Anmeldefenster angezeigt, geben Sie Ihren Windows-Benutzernamen und Ihr Kennwort für den Core-Server ein, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie auf **OK**.
4. Nach der Authentifizierung werden im linken Navigationsfenster Verknüpfungen für die Tasks angezeigt, zu deren Ausführung Sie berechtigt sind, z. B. Erstellen von Abfragen, Fernsteuerung von Clients, Verteilen von Software und Anzeigen von Berichten.

Wenn Sie den URL zu den Webkonsolenseiten nicht kennen
Wenden Sie sich an die Person, die die Webkonsole installiert hat, wahrscheinlich ist dies der Netzwerkadministrator Ihres Unternehmens.

Wenn nicht alle Verknüpfungen im linken Navigationsfenster angezeigt werden

Dies liegt wahrscheinlich daran, dass der Netzwerkadministrator die rollenbasierte Administration oder die Option "Sicherheit auf Funktionsebene" in LANDesk Management Suite verwendet, wodurch Sie an der Ausführung bestimmter Tasks gehindert werden, für die Sie eigentlich Rechte besitzen. Weitere Informationen zur rollenbasierten Administration und zur Sicherheit auf Funktionsebene finden Sie unter "Stufe 6: Installieren der Webkonsole" im *Installations- und Verteilungshandbuch.*

Erste Schritte

Anmeldung

Benutzer authentifizieren sich stets bei der Webkonsole mithilfe eines Windows NT-Kontos. Die Konten, die auf die Webkonsole zugreifen können, werden durch die Access Control Lists (ACLs) gesteuert, die in den Verzeichnissen der Webkonsole gespeichert sind. Die Webkonsolendateien befinden sich im Verzeichnis inetpub\wwwroot\remote; wenn ein Benutzer auf diese Dateien zugreifen kann, ist der Zugang und die Verwendung der Webkonsole möglich.

In den folgenden Abschnitten werden diese Fragen ausführlicher beschrieben:

- Benutzerverwaltung bei der Kommunikation mit einem Core Server
- Benutzerverwaltung bei der Kommunikation mit einem Rollup-Core
- Benutzerverwaltung für den Fall, dass sich der Core/Rollup-Server und die Webkonsole nicht auf demselben Server befinden

Benutzerverwaltung bei der Kommunikation mit einem Core Server

Wenn die Webkonsole so konfiguriert ist, dass sie die Datenbank verwendet, benutzt sie dieselbe Benutzerrolle und dieselbe Bereichsverwaltung wie die Management Suite-Konsole. Das bedeutet, dass die Benutzerrollen und -bereiche auf der Management Suite-Konsole erstellt und verwaltet werden.

Wenn ein Benutzer auf die Webkonsole zugreift, der über kein Konto auf der Management Suite-Konsole verfügt, wird ein Management Suite-Benutzerkonto erstellt mithilfe der Standardrechte und -bereiche, wie sie auf der Management Suite-Konsole konfiguriert wurden. Der Administrator kann die Rechte und Bereiche für diesen Benutzer zu einem späteren Zeitpunkt mithilfe der Management Suite-Konsole ändern.

Die in der Datenbank definierten Rechte und Bereiche überschreiben die lokalen Gruppenmitgliedschaften von Windows NT. Das bedeutet, dass sogar dann, wenn ein Benutzer zur Gruppe rc_user zugewiesen wurde (Sicherheit auf Funktionsebene), er über Fernsteuerungsrechte in der Management Suite verfügen muss, um die Fernsteuerung verwenden zu können.

Benutzerverwaltung bei der Kommunikation mit einem Rollup-Core

Die Management Suite-Konsole verwendet nicht die Rollup-Datenbank; nur die Webkonsole verwendet sie. Das bedeutet, dass der Rollup-Core lokale Gruppen verwendet, um Rechte zu steuern. Auf der Webkonsole können Sie keinen Bereich für einen Rollup-Core Server definieren. Weitere Informationen finden Sie unter "Einrichten der Sicherheit auf Funktionsebene für Rollup-Datenbanken".

Benutzerverwaltung für den Fall, dass sich der Core/Rollup-Core und die Webkonsole nicht auf demselben Server befinden

Wenn sich der Core/Rollup-Core und die Webkonsole auf verschiedenen Servern befinden, wird die gesamte Benutzerauthentifizierung bei der Webkonsole mithilfe von Windows NT-Domänenkonten vorgenommen. Außerdem müssen der Webkonsole Delegationsrechte in der Domäne zugewiesen werden.

Der Grund hierfür ist, dass die Webkonsole auf die Registrierung und die LDMAIN-Freigabe auf dem Core Server zugreifen muss. Dieser Zugriff ist nur möglich, wenn das für die Authentifizierung bei der Webkonsole verwendete Konto auf dem Core Server gültig ist. Wenn ein lokales Konto auf der Webkonsole verwendet würde, wäre eine Authentifizierung beim Core Server nicht möglich. Daher sind Windows NT-Domänenkonten erforderlich.

Auswählen eines Core Servers

Wenn Ihre Webkonsole mit einem einzigen Core Server verbunden ist, werden Sie durch Klicken auf **Anmelden** im linken Navigationsfenster erneut bei diesem Server angemeldet. Ist eine Verbindung zu mehreren Core Servern möglich, wählen Sie einen verfügbaren Core Server aus der Liste **Core** aus und klicken Sie auf **Verbinden**. Besteht noch keine Verbindung zum Server, sind gegebenenfalls Ihre Windows-Berechtigungsnachweise für die Authentifizierung erforderlich.

Weitere Informationen über den Anmeldevorgang der Webkonsole finden Sie unter "Anmelden bei der Webkonsole".

Weitere Informationen über das Konfigurieren der Webkonsole zur Verbindung mit mehreren Core Servern finden Sie unter "Konfigurieren der Webkonsole für mehrere Core Server".

Suchen eines Clients

Um einen bestimmten Client, der in der Datenbank gescannt wurde, zu suchen, verwenden Sie die Schaltfläche **Computer suchen**, die Sie jeweils oben auf der Webseite finden. Wählen Sie aus der Dropdown-Liste eine Kennung aus, z. B. **Gerätename**. Geben Sie in das Textfeld entsprechende Informationen für den gesuchten Client ein und klicken Sie anschließend auf **Suchen**.

Wenn Ihnen Name oder Adresse des Clients nur zum Teil bekannt sind, verwenden Sie im Textfeld ein Platzhalterzeichen, um alle Clients anzuzeigen, die mit Ihrem Eintrag übereinstimmen. Sie können ein Sternchen (*) oder Prozentzeichen (%) als Platzhalter verwenden. Sternchen werden nur deshalb unterstützt, weil sie einfach zu verwenden sind. Die Webkonsole ersetzt die Sternchen in Übereinstimmung mit den Konventionen der SQL-Abfragesprache durch Prozentzeichen.

Wird nur ein Client gefunden, wird eine Inventarzusammenfassung mit den Inventardaten des entsprechenden Clients angezeigt. Werden mehrere Clients gefunden, werden diese in einer Liste angezeigt. Sie zeigen die Inventarzusammenfassung eines Clients an, indem Sie auf den Namen des Clients klicken.

Wählen Sie beim Suchen eines Clients aus folgenden Kennungen aus:

- **Gerätename:**Computername des gesuchten Clients.
- **IP-Adresse:**IP-Adresse des gesuchten Clients.
- **Modell:** Das vom Inventarscanner zurückgegebene Computermodell. Das Modell kann u. U. vom Scanner nicht identifiziert werden.
- **Anzeigename:**Beschreibender Name für einen Client, z. B. Admin Platz1 – 2. Stock.
- **Anmeldename:** Anmeldename des Benutzers, dessen Computer Sie suchen. Ist der Benutzer in der Datenbank vorhanden, so werden alle mit dem Anmeldenamen verknüpften Computer angezeigt.
- **Gerätekennung:**Eindeutige Kennung, die der Inventarscanner jedem Client in der Datenbank zuweist.

Hinzufügen von Clients zum Zielwagen

Mit dem Zielwagen können Sie Software an eine bestimmte Gruppe von "Ziel"-Clients verteilen, ohne eine Abfrage für diese Gruppe erstellen zu müssen. Die Anzahl der Clients, die Sie zum Zielwagen hinzufügen, sollte 250 nicht überschreiten. Die Clients bleiben so lange "im" Wagen, bis ein Timeout bei der Webkonsolensitzung auftritt (standardmäßig nach 20 Minuten).

Sobald der Zielwagen Clients enthält, können Sie mit dem Softwareverteilungsassistenten Software an diese Clients verteilen. Alle Clients im Zielwagen empfangen das Softwarepaket.

Fügen Sie mit der Funktion **Computer suchen**, die sich oben auf jeder Webkonsolenseite befindet, der Zielwagenliste Clients hinzu. Verwenden Sie das Platzhalterzeichen % oder *, um einen bestimmten oder mehrere Clients zu suchen.

Wird nur ein Client gefunden, wird die Seite **Inventarzusammenfassung** für diesen Client angezeigt. Klicken Sie in der Symbolleiste auf die Schaltfläche **Gerät hinzufügen**, um den Client der Zielwagenliste hinzuzufügen.

Werden mehrere Clients gefunden, wählen Sie diejenigen aus, die Sie zum Zielwagen hinzufügen möchten, und klicken Sie auf **Zum Zielwagen hinzufügen**. Wenn sich die zurückgegebene Clientliste über mehrere Seiten erstreckt, klicken Sie für jede einzelne Seite auf **Zum Zielwagen hinzufügen**. Es ist nicht möglich, Clients auf mehreren Seiten auszuwählen und anschließend nur einmal für alle Seiten auf **Zum Zielwagen hinzufügen** zu klicken.

Es erscheint in jedem Fall das Fenster **Zielwagen** mit den der Liste hinzugefügten Clients. Klicken Sie auf **Fenster schließen**.

Wenn sich ein oder mehrere Clients im Zielwagen befinden, wählen Sie während des Ausführens des Softwareverteilungsassistenten **Zielwagen verwenden**, um ein Paket an diese Clients zu verteilen. Dadurch erübrigt sich eine Abfrage.

Verwenden der Fernsteuerung

Um die Fernsteuerung über die Webkonsole verwenden zu können, müssen Sie zunächst den Remote Control Viewer installieren. Sie benötigen Administratorrechte auf dem lokalen Computer, um den Viewer zu installieren. Wenn Sie die Fernsteuerungsseite zum ersten Mal aufrufen, werden Sie aufgefordert, den Viewer einzurichten.

Der Viewer funktioniert auf Windows 95/98- und Windows NT/2000/2003/XP-Computern, auf denen Internet Explorer 5.5 oder höher ausgeführt wird. Darüber hinaus muss der Fernsteuerungsagent auf allen Clients installiert werden, die gesteuert werden sollen. Sollte es später erforderlich sein, können Sie den Remote Control Viewer über die Systemsteuerung und den Befehl zum Hinzufügen bzw. Entfernen von Programmen deinstallieren. Suchen Sie in der Liste der Programme nach "Remote Control Viewer".

So verwenden Sie die Fernsteuerung für einen Client

1. Klicken Sie im linken Navigationsfenster auf **Fernsteuerung**.
2. Geben Sie im leeren Textfeld den Namen oder die IP-Adresse des Clients ein, der gesteuert werden soll, und klicken Sie auf **Fernsteuerung**. Damit wird eine Fernsteuerungssitzung gestartet. Wenn Sie Ihren Browser nach dem Start der Sitzung schließen, wird die Sitzung weiterhin ausgeführt.

Sie können auch Computer fernsteuern, die nicht in die Datenbank gescannt wurden (sofern ein Fernsteuerungsagent darauf installiert ist). Außerdem können mehrere Computer gleichzeitig ferngesteuert werden. Nachdem Sie eine Sitzung gestartet haben, kehren Sie zur Webkonsole zurück, geben den Namen oder die IP-Adresse eines anderen Computers ein und klicken auf **Fernsteuerung**.

Aktivieren eines Clients

Wenn Ihre Clients die Wake-on-LAN*-Technologie unterstützen, können Sie die Webkonsole für eine Fernaktivierung der Clients verwenden. Diese Funktion ist hilfreich, wenn Sie einen derzeit ausgeschalteten Client fernsteuern bzw. ein Softwaredistributionspaket an ihn senden möchten.

Beim Aktivieren eines Clients wird ein Paket der Wake-on-LAN-Technologie an den Netzwerkadapter dieses Clients gesendet. Sind Netzwerkadapter und Client Wake on LAN-fähig, wird der Client gestartet. Andernfalls bleibt der Client ausgeschaltet.

Um eine Fernaktivierung eines Clients durchzuführen, müssen Sie ihn zunächst in der Datenbank suchen. Verwenden Sie dazu die Funktion **Computer suchen** am oberen Rand der Webkonsolenseite. Sobald Sie den Client gefunden haben, können Sie ihn auf der Seite "Inventarzusammenfassung" aktivieren, indem Sie in der Symbolleiste auf das Symbol **Wake on LAN** klicken.

Installieren und Konfigurieren von Clients

Auswählen von Clientfunktionen

Um Clients mithilfe der Webkonsole verwalten zu können, müssen Management-Agenten auf den Clients installiert werden. Management-Agenten werden mithilfe eines Clientagent-Pakets (ausführbare Einzeldatei) installiert. Die Clients installieren die Agenten, indem sie ein von Ihnen erstelltes Clientkonfigurationspaket ausführen.

Die Webkonsole bietet nur eine beschränkte Unterstützung für Clientkonfigurationspakete
Die Webkonsole erstellt nur einfache Konfigurationspakete, die mit den nachstehend genannten Funktionen ausgestattet sind. Um Clientkonfigurationen zu erstellen, die andere Funktionen einschließen, oder um Funktionsoptionen anzupassen, verwenden Sie die Clientsetup-Option der Management Suite-Konsole (**Extras | Clientsetup**).

Clients, die von Ihnen zum ersten Mal konfiguriert werden, müssen das Paket manuell ausführen. Das Paket blendet keine Benutzerabfragen ein. Sobald Sie den Softwaredistribution-Agenten auf Clients installiert haben, können Sie die Management-Agenten auf den betreffenden Clients aktualisieren, indem Sie ein neues Paket erstellen und es mithilfe der Softwaredistribution installieren. Clients, die die Fernsteuerungs- oder Softwaredistribution-Agenten zum ersten Mal erhalten, werden nach Abschluss der Paketinstallation aufgefordert, einen Neustart durchzuführen.

Verwenden Sie die Clientkonfigurationsseite, um einem Clientkonfigurationspaket einen Namen zuzuweisen und um die Funktionen auszuwählen, die in dem Paket enthalten sein sollen. Die folgenden Funktionen stehen zur Auswahl.

- **Fernsteuerung:** Aktivieren Sie diese Option, wenn Sie Clients fernsteuern möchten.
- **Inventarscanner: Aktivieren Sie diese Option, wenn Sie veranlassen möchten, dass Clients Inventardaten an den Core Server übermitteln.**Anschließend können Sie dann Abfragen in den Inventardaten durchführen. Der Inventarscanner fügt Clients zur Datenbank hinzu, damit Sie diese von der Webkonsole aus verwalten können. Mit dieser Funktion lassen sich auch benutzerdefinierte Datenformulare verteilen.
- **Enhanced Software Distribution:** Aktivieren Sie diese Option, wenn Sie Software an Clients verteilen möchten. Sie können einzelne Dateien oder ausführbare Einzeldateien verteilen. Für die ausführbare Einzeldatei gilt, dass der Client das Programm ausführt, sobald ihm die Einzeldatei zugestellt wird.
- **Softwarelizenzüberwachung:** Aktivieren Sie diese Option, wenn Sie die Softwareverwendung auf Clients überwachen möchten. Sie können zu überwachende Anwendungen konfigurieren und die gesammelten Informationen von den Clients an die Inventardatenbank übermitteln lassen.

So beginnen Sie mit der Erstellung eines Clientkonfigurationspakets

1. Geben Sie einen **Dateinamen** für das Paket ein. Sobald die Webkonsole das Paket erstellt hat, wird es im Ordner "\Program Files\LANDesk\ManagementSuite" auf dem Core Server gespeichert.

2. Aktivieren Sie die Funktionen, die vom Paket installiert werden sollen.
3. Klicken Sie auf **Weiter**, um die Clientfunktionen zu konfigurieren.

Installieren von Clientagenten

Nachdem Sie eine Clientkonfiguration in der Webkonsole erstellt haben, müssen Sie diese auf den entsprechenden Clients installieren. Welche Methode sich am besten für die Installation von Clientagenten eignet, hängt davon ab, ob Sie die Agenten zum ersten Mal installieren oder eine vorhandene Clientagentinstallation aktualisieren.

Bei den Clientagentenpaketen handelt es sich um selbstextrahierende ausführbare Dateien. Standardmäßig werden diese Dateien im Ordner "\Program Files\LANDesk\ManagementSuite" auf dem Core Server gespeichert. Durch Starten der ausführbaren Datei werden die Clientagenten ohne Benutzerabfragen im Hintergrund installiert.

Wenn Sie dasselbe Clientagentpaket mehr als einmal auf einem Client ausführen, wird ein Dialogfeld eingeblendet, in dem Sie gefragt werden, ob Sie das Paket neu installieren oder reparieren möchten. Bei einer Neuinstallation des Pakets werden alle Dateien erneut kopiert. Wenn Sie das Paket reparieren, werden nur die geänderten Dateien kopiert. Jede der beiden Optionen lässt sich problemlos verwenden.

Erste Installation eines Agenten

Wenn Benutzer das Clientagentpaket zum ersten Mal installieren, müssen sie während der Installation mit einem Konto angemeldet sein, das über administrative Rechte verfügt. Die Clientagenten lassen sich mit einem Konto, das keine administrativen Rechte besitzt, nicht installieren. Wenn Ihre Benutzer sich für die Installation des Pakets nicht mit administrativen Rechten anmelden können, muss ein Benutzer, der über solche Rechte verfügt, die Installation übernehmen.

Sie können das Clientagentpaket Clients zur Verfügung stellen, indem Sie es auf einem Dateiserver oder einem Webserver ablegen.

Aktualisieren vorhandener Agenten

Wenn eine vorhandene Clientagentinstallation die Funktionalität zur Softwareverteilung einschließt, können Sie die Agenten aktualisieren, indem Sie eine neue Clientkonfiguration erstellen und von der Webkonsole aus verteilen. Hiermit werden die Agenten im Hintergrund installiert. In diesem Fall müssen die Benutzer während der Installation des Agenten nicht mit administrativen Privilegien angemeldet sein.

Sobald Sie ein Clientagentpaket installiert haben, werden beim Installieren weiterer Clientagentpakete nur noch Agents zu den Clients hinzugefügt. Sie können keinen Agent deinstallieren, indem Sie ein neues Clientagentpaket erstellen, in dem der zu entfernende Agent nicht enthalten ist.

Nachdem Sie ein neues Clientagentpaket erstellt haben, kopieren Sie es auf den Delivery-Server für Verteilungspakete. Weitere Informationen finden Sie unter "Einrichten eines Delivery-Servers für Verteilungspakete".

Deinstallieren von Agenten

Agenten können mit dem nachstehend beschriebenen Verfahren von Clients deinstalliert werden.

So deinstallieren Sie Agenten von einem Client

1. Melden Sie sich mit administrativen Rechten beim Client an.
2. Ordnen Sie der LDLOGON-Freigabe des Core Servers ein Laufwerk zu.
3. Öffnen Sie eine Befehlsaufforderung, wechseln Sie zum Laufwerksbuchstaben der LDLOGON-Freigabe und geben Sie Folgendes ein:

```
wscfg32 /f /n /u
```

4. Die Deinstallation wird im Hintergrund ausgeführt und startet, nachdem sie vollständig ausgeführt wurde, den Client neu.

Verwalten von Inventardaten

Erstellen benutzerdefinierter Abfragen

Benutzerdefinierte Abfragen sind nützlich, wenn Sie Inventardetails über auf den Clientcomputern installierte Hardware und Software wissen möchten. Verwenden Sie eine benutzerdefinierte Abfrage dazu, eine Liste mit Clients mit ähnlichem Inventar zusammenzustellen. Wenn Sie beispielsweise Clients auf einen Prozessor mit 750 MHz aufrüsten möchten, können Sie alle Computer mit einer Prozessorgeschwindigkeit unter 750 MHz in der Datenbank abfragen.

Sie können alle Inventarelemente (die so genannten "Attribute") abfragen, die der Inventarscanner in der Datenbank speichert.

Zum Erstellen einer Abfrage sind vier Schritte erforderlich:

1. **Eine Suchbedingung erstellen:** Geben Sie eine Reihe von Inventarattributen an, die die Grundlage der Abfrage bilden.
2. **Attribute zum Anzeigen auswählen:** Verfeinern oder "filtern" Sie die Abfrage so, dass die Ergebnisse die für Sie nützlichsten Attribute anzeigen, wie z. B. IP-Adressen oder Gerätenamen.
3. **Ergebnisse nach Attributen sortieren (optional):** Geben Sie an, wie die Abfrageergebnisse sortiert werden sollen. (Dies trifft nur zu, wenn Sie in Schritt 2 mehr als einen Attributtyp zur Anzeige in den Abfrageergebnissen ausgewählt haben.)
4. **Abfrage ausführen:** Führen Sie die soeben erstellte Abfrage aus. Sie können sie auch zur späteren Verwendung speichern oder alle Abfragedaten löschen und eine neue Abfrage erstellen.

Schritt 1: Erstellen einer Suchbedingung

Eine Suchbedingung besteht aus einer Reihe von Inventarattributen und verknüpften Werten, die Sie abfragen. Als Grundlage für eine Abfrage können Sie eine Suchbedingung verwenden oder mehrere Suchbedingungen zu einer Gruppe zusammenstellen.

Die folgenden Schritte führen Sie auf der Seite Abfrage bearbeiten aus.

So erstellen Sie eine Suchbedingung

1. Klicken Sie in Schritt 1 auf **Bearbeiten**. Es wird ein Fenster mit einer Liste angezeigt, die alle momentan in der Datenbank vorhandenen Inventardaten enthält.
2. Wählen Sie die Attribute in der Liste aus, die Sie als Suchbedingung festlegen möchten. Um beispielsweise alle Clients zu suchen, die eine bestimmte Software ausführen, wählen Sie Computer.Software.Paket.Name.
3. Nach dem Auswählen der Attribute wird auf der rechten Seite des Fensters eine Reihe von Feldern angezeigt. Wählen Sie aus diesen Feldern einen Operator und Wert aus, um die Suchbedingung zu vervollständigen. Um beispielsweise alle Clients zu suchen, die Internet Explorer 5.0 ausführen, geben Sie als Attribute "Computer.Software.Paket.Name", als Operator "=" und als Wert "Internet Explorer 5" ein.

4. Klicken Sie am unteren Fensterrand auf **Hinzufügen**, um das leere Feld mit der Suchbedingung auszufüllen.
5. Sie können die Abfrage weiter spezifizieren, indem Sie eine weitere Suchbedingung erstellen und sie der ersten Bedingung mit einem Booleschen Operator (AND oder OR) hinzufügen. Über die Schaltflächen können Sie Bedingungen hinzufügen, löschen, ersetzen, gruppieren oder die Gruppierung aufheben.
6. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.

Schritt 2: Auswählen der anzuzeigenden Attribute

In Schritt 2 wählen Sie Attribute aus, die besonders nützlich sind, um die in den Abfrageergebnissen zurückgegebenen Computer zu identifizieren. Wenn Sie anhand der Ergebnisse beispielsweise jeden Computer, der den in Schritt 1 angegebenen Suchbedingung entspricht, physikalisch orten möchten, geben Sie Attribute wie den Anzeigenamen des Computers (Computer.Anzeigename) oder die IP-Adresse (Computer.Netzwerk.TCPIP.Adresse) an.

Die folgenden Schritte führen Sie auf der Seite **Abfrage bearbeiten** aus.

So wählen Sie Attribute zum Anzeigen aus

1. Klicken Sie in Schritt 2 auf **Bearbeiten**. Es wird ein Fenster mit einer Liste angezeigt, die alle momentan in der Datenbank vorhandenen Inventardaten enthält.
2. Wählen Sie ein Attribut in der Liste aus, das in der Abfrageergebnisliste angezeigt werden soll. Wählen Sie dabei Attribute aus, mit denen Sie die in der Abfrage zurückgegebenen Clients identifizieren können.

   Hinweis: Wenn Sie eine Oracle-Datenbank verwenden, wählen Sie mindestens ein Attribut aus, das direkt durch den Inventarscanner definiert ist (z. B. Computer.Anzeigename, Computer.Gerätename, Computer.Gerätekennung, Computer.Anmeldename usw.).
3. Klicken Sie nach dem Auswählen eines Attributs auf **>>**, um es in das leere Feld auf der rechten Seite des Fensters zu verschieben. Wenn Sie die Abfrageergebnisse in der Liste nummerieren möchten, klicken Sie auf **Anzahl aufnehmen**.
4. Beenden Sie den Vorgang, wenn Sie nur ein Attribut anzeigen möchten, oder fahren Sie fort, um weitere Attribute hinzuzufügen. Verwenden Sie die Pfeiltasten, um Attribute hinzuzufügen oder zu entfernen. Wenn Sie die Reihenfolge der Attribute ändern möchten, klicken Sie auf **Nach oben** bzw. **Nach unten**. Um Gesamtsummen der Ergebnisse anzuzeigen, klicken Sie auf **Anzahl hinzufügen** bzw. **Anzahl entfernen**.
5. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.

Der Abfrageergebnisliste können Sie auch Spaltenüberschriften hinzufügen.

So fügen Sie Spaltenüberschriften hinzu

1. Klicken Sie in Schritt 2 auf **Spaltenüberschriften bearbeiten**.
2. Geben Sie im Feld **Spaltenüberschriften** eine Spaltenüberschrift ein, und klicken Sie auf **Hinzufügen**. Geben Sie für jede Spalte der Ergebnisliste eine Überschrift ein. Die Anzahl der Spalten hängt von der Anzahl der Attribute ab, die Sie für die Ergebnisliste angegeben haben.
3. Klicken Sie auf **OK**.

Speichern Sie nun gegebenenfalls die Abfrage. Der nächste Schritt im Abfrageerstellungsprozess ist optional und gilt nur für Abfrageergebnisse, die zwei oder mehr Spalten enthalten. Klicken Sie zum Speichern der Abfrage auf **Abfrage speichern** unten auf der Seite. Es wird ein Fenster angezeigt und Sie werden zur Eingabe eines Namens für diese Abfrage aufgefordert. Geben Sie einen Namen ein, und klicken Sie anschließend in der rechten oberen Ecke des Fensters auf **Speichern**.

Schritt 3: Sortieren der Ergebnisse nach Attribut

Dieser Schritt ist nur notwendig, wenn Sie in Schritt 2 mehr als ein Attribut oder Spaltenüberschrift definiert haben und die Ergebnisse alphabetisch oder nummerisch innerhalb einer Spalte sortieren möchten.

Angenommen, Sie haben zwei verschiedene Attribute angegeben, die in den Abfrageergebnissen angezeigt werden sollen: die IP-Adresse und den Prozessortyp des zurückgegebenen Computers. In Schritt 3 können Sie die Ergebnisse alphabetisch nach Prozessortyp sortieren.

Wenn Sie diesen Schritt überspringen, wird die Abfrage automatisch nach dem ersten, in Schritt 2 gewählten Attribut sortiert.

So sortieren Sie die Ergebnisse nach Attribut

1. Klicken Sie in Schritt 3 auf **Bearbeiten**. Ein Fenster mit den in Schritt 2 gewählten Attributen wird geöffnet.
2. Wählen Sie das Attribut, nach dem sortiert werden soll, und klicken Sie anschließend auf **>>**, um es in das leere Textfeld zu verschieben.
3. Klicken Sie auf **OK**.

Schritt 4: Ausführen der Abfrage

Nach Erstellen einer Abfrage können Sie diese ausführen, speichern oder löschen und eine neue Abfrage erstellen.

Um die Abfrage für eine zukünftige Verwendung zu speichern, klicken Sie in der Symbolleiste auf die Schaltfläche **Speichern**. Die Abfrage wird nun in der Liste auf der Seite **Benutzerdefinierte Abfragen** angezeigt. Handelt es sich bei der Abfrage um eine geänderte Version einer anderen Abfrage, klicken Sie in der Symbolleiste auf die Schaltfläche **Speichern unter**, um sie umzubenennen.

Standardmäßig sind gespeicherte Abfragen nur für den Benutzer sichtbar, der sie gespeichert hat. Wenn Sie vor dem Speichern das Kontrollkästchen **Öffentliche Abfrage** aktivieren, ist die Abfrage für alle Benutzer sichtbar.

Die Management Suite-Konsole und die Webkonsole verwenden Abfragen gemeinsam. Wenn Sie eine Abfrage in der Management Suite-Konsole speichern, wird sie auch in der Webkonsole angezeigt und umgekehrt.

Zum Anzeigen der Ergebnisse dieser Abfrage klicken Sie in der Symbolleiste auf die Schaltfläche **Ausführen**.

Um die Abfrageparameter auf der Seite **Abfrage bearbeiten** zu löschen, klicken Sie in der Symbolleiste auf die Schaltfläche **Löschen**. Wurde die Abfrage bereits gespeichert, wird sie auf dieser Seite gelöscht, bleibt aber in der Liste **Benutzerdefinierte Abfragen** gespeichert.

Exportieren und Importieren von Abfragen

Mit der Webkonsole erstellte Abfragen lassen sich exportieren und importieren. Alle Abfragen werden als XML-Dateien exportiert. Wenn Sie eine Abfrage mit demselben Dateinamen mehr als einmal exportieren, wird die Datei überschrieben. Um dies zu verhindern, können Sie die Datei nach dem Exportieren an einen anderen Speicherort kopieren.

Die Funktionen zum Exportieren und Importieren sind in zwei Szenarien nützlich:

- Wenn Sie Ihre Datenbank erneut installieren müssen, verwenden Sie die Export- und Importfunktionen, um Ihre vorhandenen Abfragen für die Verwendung in einer neuen Datenbank zu speichern.

  Sie können die Abfragen beispielsweise exportieren und anschließend in ein Verzeichnis verschieben, das von einer Datenbankneuinstallation nicht betroffen ist. Nachdem Sie die Datenbank neu installiert haben, können Sie die Abfragen wieder in das Abfrageverzeichnis auf Ihrem Webserver verschieben und anschließend in die neue Datenbank importieren.

- Sie können die Export-/Importfunktionen verwenden, um Abfragen in andere Datenbanken zu kopieren. (Dies ist nützlich, wenn das System nicht zum Anzeigen von zwei oder mehr Datenbanken mit der Webkonsole eingerichtet ist.)

  Sie können beispielsweise eine Abfrage in ein Abfrageverzeichnis auf dem Webserver exportieren und anschließend per E-Mail oder FTP an einen anderen Benutzer senden. Dieser Benutzer kann die Abfragen dann in ein Abfrageverzeichnis auf einem anderen Webserver speichern und anschließend in eine Datenbank importieren. Sie können auch ein Laufwerk zuweisen und die Abfragen direkt in das Abfrageverzeichnis eines anderen Webservers kopieren.

So exportieren Sie eine Abfrage

Führen Sie folgende Schritte aus, während Sie mit einer Datenbank verbunden sind, in der sich die zu exportierende Abfrage befindet.

1. Klicken Sie im linken Navigationsfenster auf **Inventar > Benutzerdefinierte Abfragen**.
2. Klicken Sie auf der Seite "Benutzerdefinierte Abfragen" auf den Namen der zu exportierenden Abfrage.
3. Klicken Sie auf der Seite "Abfrage bearbeiten" auf die Symbolleistenschaltfläche **Exportieren**, um die Abfrage auf die Festplatte zu exportieren.
4. Klicken Sie auf der Seite "Abfrage exportiert" mit der rechten Maustaste auf die Abfrage, um sie als XML-Datei in einem ausgewählten Verzeichnis zu speichern. Die Abfrage wird nun zu einer XML-Datei.

Wenn Sie eine Abfrage mehr als einmal exportieren, wird die Datei überschrieben. Um dies zu verhindern, können Sie die Datei nach dem Exportieren an einen anderen Speicherort kopieren.

Wenn Sie die Abfrage wieder in eine Datenbank importieren möchten, verschieben Sie sie in das Abfrageverzeichnis, das vom Webserver erkannt wird (standardmäßig c:\inetpub\wwwroot\remote\queries).

So importieren Sie eine Abfrage

Führen Sie folgende Schritte aus, während Sie mit der Datenbank verbunden sind, in die Sie eine Abfrage importieren möchten.

1. Klicken Sie im linken Navigationsfenster auf **Inventar > Benutzerdefinierte Abfragen**.
2. Klicken Sie auf der Seite "Benutzerdefinierte Abfragen" auf **Neue Abfrage**.
3. Klicken Sie auf der Seite "Abfrage bearbeiten" auf die Symbolleistenschaltfläche **Importieren**. Wenn Sie ursprünglich mehrere Abfragen gleichzeitig exportiert haben, klicken Sie auf die Symbolleistenschaltfläche **Alle importieren**.
4. Wählen Sie die Abfrage aus, die Sie importieren möchten. Wenn Sie die Parameter dieser Abfrage vor dem Importieren überprüfen möchten, klicken Sie auf **Ansicht**.
5. Klicken Sie auf **Importieren**, um die Abfrage auf die Seite "Abfrage bearbeiten" zu laden.
6. Blättern Sie, sobald die Abfrage geladen ist, nach unten, und klicken Sie auf **Abfrage speichern**, um die Abfrage in dieser Datenbank zu speichern.

Kopieren von Abfragen zwischen Core Servern

Ist die Webkonsole für die Anzeige mehrerer Core Server eingerichtet, können Sie Abfragen von einem Core Server auf einen anderen kopieren, indem Sie die nachfolgenden Schritte ausführen.

Ist die Webkonsole nicht für die Anzeige mehrerer Core Server eingerichtet, kopieren Sie Abfragen mit der Export- und Importfunktion.

So kopieren Sie ein Abfrage von einem Core Server auf einen anderen

Stellen Sie eine Verbindung zu dem Core Server her, vom dem Sie eine Abfrage kopieren möchten, und führen Sie folgende Schritte aus.

1. Klicken Sie im linken Navigationsfenster auf **Inventar > Benutzerdefinierte Abfragen**.
2. Laden Sie die zu kopierende Abfrage von der Seite **Benutzerdefinierte Abfragen**, indem Sie auf den entsprechenden Namen in der Liste klicken.
3. Prüfen Sie auf der Seite **Abfrage bearbeiten**, ob die Abfrage tatsächlich geladen ist.
4. Klicken Sie im linken Navigationsfenster auf **Anmelden**, und melden Sie sich bei einer anderen Datenbank an.
5. Klicken Sie im linken Navigationsfenster auf **Inventar > Benutzerdefinierte Abfragen**.
6. Klicken Sie auf der Seite **Benutzerdefinierte Abfragen** auf **Aktuelle bearbeiten**.
7. Prüfen Sie auf der Seite **Abfrage bearbeiten**, ob die von dem anderen Core Server stammende Abfrage geladen ist.
8. Blättern Sie nach unten, und klicken Sie auf **Abfrage speichern unter**, um die Abfrage auf diesem Core Server zu speichern.

Exportieren von Abfrageergebnissen in CSV-Dateien

Um die Ergebnisdaten Ihrer Abfrage in einem Tabellenkalkulationsprogramm anzuzeigen, exportieren Sie die Daten als Datei mit kommagetrennten Werten (CSV-Datei). Klicken Sie auf der Seite "Abfrageergebnisse" in der Symbolleiste auf die Schaltfläche **Speichern unter CSV**, um Ihre Daten als CSV-Datei zu speichern.

Anschließend können Sie die CSV-Datei in ein Tabellenkalkulationsprogramm wie Microsoft Excel* importieren und dort bearbeiten.

Anzeigen von Berichten

Die Berichte bieten Ihnen die Möglichkeit, schnell auf eine grafische Darstellung des Informationsguthabens auf Ihren Clientcomputern zuzugreifen. Die Berichte werden aus den Daten zusammengestellt, die der Scanner in der Datenbank speichert. Berichte können angezeigt, gedruckt und per E-Mail weitergeleitet werden.

So zeigen Sie einen Bericht an

1. Klicken Sie im linken Navigationsfenster auf **Inventar Berichte**. Berichtkategorien werden im rechten Fensterausschnitt angezeigt. Klicken Sie auf die Überschrift einer Kategorie, um die Liste mit den Berichten anzuzeigen. Neben dem jeweiligen Bericht zeigt ein Symbol an, um welchen Berichttyp es sich handelt.

   Ein Bericht, neben dem ein Diagrammsymbol zu sehen ist, wird als Torten- oder Balkendiagramm angezeigt. Sie können in einem Diagramm auf jeden farbigen Balken oder Tortenausschnittklicken, um einen Drilldown zu einer Übersicht auszuführen.

   Ein Bericht mit einem Dokumentsymbol wird als Text angezeigt.

2. Klicken Sie auf den Berichtnamen, um den Bericht anzuzeigen.

3. Für die Hardware- oder Softwarescan-Datumsübersicht klicken Sie auf das jeweilige Start- und Enddatum, um den Zeitrahmen festzulegen. Klicken Sie anschließend auf **Ausführen**.

Berichte lassen sich ausdrucken, indem Sie mit der rechten Maustaste auf die Seite und dann auf **Drucken** klicken. Klicken Sie im Dialogfeld "Drucken" auf **Drucken**. Wenn sich ein Bericht über mehrere Seiten erstreckt, klicken Sie mit der rechten Maustaste auf jede Seite, um sie zu drucken.

Einen Bericht, den Sie per E-Mail weiterleiten möchten, sollten Sie in eine PDF-Datei drucken, die Sie dann der E-Mail als Anhang beifügen.

Die Webkonsole zeigt Berichtdiagramme als Torten- oder Balkendiagramme an. Klicken Sie zur Festlegung des Diagrammtyps auf **Konfigurieren > Einstellungen**, ändern Sie anschließend den Diagrammtyp und klicken Sie auf **Aktualisieren**.

Damit die in vielen Berichten enthaltenen interaktiven Balken- und Tortendiagramme angezeigt werden, muss Macromedia Flash Player* 7 installiert sein.

Verwenden von benutzerdefinierten Formularen

Sie können ein Formular erstellen, um zusätzliche Informationen zu den gescannten Bestandsdaten hinzuzufügen. Mit den benutzerdefinierten Formularen können unternehmens- oder situationsspezifische Daten abgefragt werden.

Verwenden Sie Inventarscanner-Clientkonfigurationen, um benutzerdefinierte Formulare an Clients zu verteilen. Sie können ein Formular in die Inventarscanner-Optionen einfügen. Beim Installieren des Inventarscanners auf einem Client wird das benutzerdefinierte Formular als Teil der Clientinstallation angezeigt. Sobald ein Client das Formular ausgefüllt hat, führt der Inventarscanner das Formular aus und schickt die Formulardaten an den Core Server. Dort stehen sie für Abfragen und Berichte zur Verfügung.

Clients verwenden die Formularanzeige, um zu überprüfen, welche Formulare sie ausgefüllt haben oder noch ausfüllen müssen. Die Formularanzeige wird auf den Clients mit **Start | Programme | LANDesk Management | Benutzerdefinierte Formulare** aufgerufen. Clients können ein ihnen zugestelltes Formular auswählen. Klicken Sie dann auf **Öffnen**, um das Formular zu bearbeiten. Wenn der Inventarscanner das nächste Mal ausgeführt wird, schickt er die neuen Formulardaten an den Core Server.

Sie können die in den benutzerdefinierten Formularen enthaltenen Daten von jeder Inventarstrukturansicht aus anzeigen oder abfragen, indem Sie **Benutzerdefinierte Daten > Formulare** auswählen.

Klicken Sie auf **Verwalten > Benutzerdefinierte Formulare**, um die Seite "Benutzerdefinierte Formulare" zu öffnen. Auf dieser Seite können Sie Formulare erstellen, bearbeiten oder löschen.

- Um ein vorhandenes Formular zu bearbeiten, wählen Sie das Formular aus und klicken dann auf **Bearbeiten**.
- Um ein neues Formular zu erstellen, klicken Sie auf **Neu**. Geben Sie im Dialogfeld "Neues Formular" einen Namen für das neue Formular ein und klicken Sie auf **OK**..

- Um ein vorhandenes Formular zu löschen, wählen Sie das Formular aus und klicken dann auf **Löschen**. Sie werden aufgefordert, Ihr Vorhaben zu bestätigen.

Hinzufügen von Formularfeldern

Wenn Sie ein neues Formular erstellen oder ein vorhandenes bearbeiten, können Sie mit den Optionen auf der Seite <*Formularname*>.frm Formularfelder hinzufügen.

Klicken Sie auf **Feld hinzufügen**, um ein neues Feld zu dem benutzerdefinierten Formular hinzuzufügen. Geben Sie die Attribute für das Feld in das Formular-Dialogfeld ein und klicken Sie anschließend auf **Senden**.

- Geben Sie im Bearbeitungsfeld **Frage** das Wort oder den Satz ein, mit dem Sie den Benutzer zur Eingabe von Informationen in das Formular auffordern.
- Geben Sie im Bearbeitungsfeld "Inventarnamen" den Namen des neuen Formularfeldes ein. Der Name wird nicht im Formular angezeigt. Er ermöglicht es Ihnen jedoch, die Datenbank nach den Informationen abzufragen, die von den Benutzern in das Formular eingegeben werden.
- Geben Sie im Bearbeitungsfeld **Beschreibung** Informationen zu dem neuen Formularfeld ein. Diese Informationen werden angezeigt, wenn der Benutzer beim Ausfüllen des betreffenden Feldes auf die Schaltfläche "Hilfe" im Formular klickt.
- Wählen Sie in der Dropdown-Liste **Typ** einen Feldtyp aus. Es gibt drei verschiedene Feldtypen: Bearbeitungsfeld, Listenfeld und Kombinationsfeld. In ein Bearbeitungsfeld kann unformatierter Text eingegeben werden. Ein Listenfeld erstellt eine Dropdown-Liste mit vordefinierten Optionen. Ein Kombinationsfeld stellt Optionen zur Verfügung, gibt jedoch Benutzern zusätzlich die Möglichkeit, eine Option einzugeben, die nicht aufgelistet ist.
- Geben Sie bei der Erstellung eines Auswahlfeldes die Optionen in das Bearbeitungsfeld **Optionen** ein. Trennen Sie die Optionen durch ein Standard-ANSI-Komma voneinander. Die eingegebenen Optionen werden in der Dropdown-Liste angezeigt. Für Textfelder werden keine Optionen benötigt.
- Aktivieren Sie die Option **Steuerung ist erforderliches Feld und muss ausgefüllt werden**, wenn Sie dieses Feld als Pflichtfeld für den Benutzer konfigurieren möchten. Wenn diese Option aktiviert ist, kann der Benutzer das Formular erst senden, nachdem er das Feld ausgefüllt hat.

Klicken Sie auf **Feld bearbeiten**, um ein Feld des benutzerdefinierten Formulars zu ändern. Klicken Sie auf **Senden**, nachdem Sie alle Änderungen ausgeführt haben. Klicken Sie auf **Feld löschen**, um ein Feld aus dem benutzerdefinierten Formular zu entfernen. Mithilfe der Schaltflächen **Nach oben** und **Nach unten** können Sie die Reihenfolge der Formularfelder ändern. Klicken Sie auf **Seitenumbruch**, um einen Seitenumbruch einzufügen. Nachdem Sie einen Seitenumbruch eingefügt haben, können Sie diesen genauso wie Formularfelder nach oben oder unten verschieben oder löschen.

Klicken Sie auf **Name bearbeiten**, um die Überschrift des Formulars und die über den Formularfeldern angezeigten Anweisungen zu ändern. Klicken Sie auf **Senden**, nachdem Sie alle Änderungen ausgeführt haben.

Klicken Sie auf **Fertig**, nachdem Sie Felder zum Formular hinzugefügt haben.

Löschen von Computern aus der Datenbank

Löschen Sie Computer aus der Datenbank, indem Sie auf **Verwalten > Computer löschen** im linken Navigationsfenster klicken. Zeigen Sie von der Seite "Computer löschen" aus den Inhalt des Zielwagens an. Überprüfen Sie genau, welche Computer sich im Zielwagen befinden, bevor Sie diese aus der Datenbank löschen. Sobald Sie Inventardaten aus der Datenbank gelöscht haben, können Sie die Aktion weder rückgängig machen noch die Daten wiederherstellen.

Um alle Computer im Zielwagen aus der Datenbank zu löschen, klicken Sie auf **Löschen**. Sie werden aufgefordert, Ihr Vorhaben zu bestätigen. Jeder im Zielwagen angezeigte Computer wird gelöscht, ganz gleich, ob er im Zielwagen ausgewählt ist oder nicht.

Wenn Sie die Fehlermeldung "Kann Computer nicht löschen" erhalten.
Dieser Fehler wird angezeigt, wenn Sie versuchen, Computer aus der Datenbank zu löschen, sich aber keine Computer im Zielwagen befinden. Sie können nur Computer löschen, die Sie zuvor zum Zielwagen hinzugefügt haben.

Softwarelizenzüberwachung

Überwachen der Einhaltung von Softwarelizenzbestimmungen

Für IT-Administratoren ist es oft schwierig, den Einsatz von Produktlizenzen zu verfolgen, die auf vielen Clients innerhalb eines Netzwerks installiert sind. Sie laufen nicht nur Gefahr, Produktlizenzen zu häufig bereitzustellen, sondern auch, zu viele Lizenzen für Produkte zu kaufen, die sich als unnötig erweisen. Sie können diese Probleme vermeiden, indem Sie mithilfe der Softwarelizenzüberwachung den Einsatz von Produktlizenzen und die Verwendung von Produkten innerhalb Ihrer Organisation überwachen und die betreffenden Daten in Berichten zusammenstellen.

Die Leistungsfähigkeit dieser Überwachungsfunktion beruht auf ihren Datenerfassungsmöglichkeiten. Verwenden Sie die Daten, um die Erfüllung von Lizenzbestimmungen allgemein zu verfolgen und Trends hinsichtlich der Produktverwendung und -verweigerung zu beobachten. Der Softwarelizenzüberwachungsagent überwacht passiv die Produktverwendung auf Clients und belegt hierbei minimale Netzwerkbandbreite. Der Agent überwacht auch die Verwendung von Produkten auf mobilen Clients, die vom Netzwerk getrennt sind.

Die Überwachung umfasst folgende Funktionen:

- Die Fähigkeit, für bekannte als auch unbekannte Anwendungen zu scannen.
- Anwendungsstartverweigerung, um die Ausführung nicht autorisierter Software zu verhindern - sogar auf Clients, die nicht mit dem Netzwerk verbunden sind.
- Vollständige Integration in die Webkonsole für aktuelle, komplette Informationen über installierte Anwendungen.
- Umfassende Berichte zur Anwendungsnutzung und zu Lizenzbestimmungen.
- Umfassende Funktionen zur Lizenzüberwachung und Berichtserstellung, einschließlich Informationen darüber, wie oft jede lizenzierte Anwendung aufgerufen wurde, Datum der letzten Verwendung und Gesamtdauer der Anwendungsnutzung.
- Einfache Konfiguration der Lizenzparameter, einschließlich gekaufter Anzahl, Lizenztyp, Menge und Seriennummer.
- Informationen zum Lizenzkauf, einschließlich Preis, Kaufdatum, Auftragsnummer und Wiederverkäuferdaten.
- Installationsverfolgung und -abstimmung, einschließlich Lizenzinhaber und physikalischer Standort des Clients, auf dem die Lizenz installiert ist, sowie weitere Informationen.
- Aliasnamen zur Verfolgung von Software, wenn sich Anbieterdaten oder Dateinamen ändern.

Die Funktion zum Überwachen der Einhaltung von Softwarelizenzbestimmungen in der Webkonsole besitzt nur einen Teil des Funktionsspektrums, über das die in der Management Suite-Konsole enthaltene Version verfügt. Verwenden Sie deshalb für eine umfassende Lizenzeinhaltungskonfiguration (einschließlich entsprechend leistungsstarker Wartungs- und Berichtfunktionen) die Management Suite-Konsole.

Zur Funktionsweise der Softwarelizenzüberwachung

Der Agent für die Softwarelizenzüberwachung zeichnet, wenn er installiert ist, Daten zu allen auf einem Client installierten Anwendungen auf und speichert diese Daten in der Registrierung des Clients unter:

HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\Software Monitoring\MonitorLog

Anwendungsverwendungsdaten, die nicht von Ihnen überwacht werden, werden in der Registrierung des Clients schließlich durch neuere Daten überschrieben.

Der Client-Inventarscanner aktualisiert den Core Server während der Durchführung des Softwarescans mit Softwarelizenzüberwachungsdaten (standardmäßig einmal pro Tag). Der Inventarscanner bestimmt anhand einer Textdatei mit dem Namen LDAPPL3.INI, welche Anwendungen er scannen muss. Wenn der Inventarscanner ausgeführt wird, informiert er sich beim Core Server, ob die LDAPPL3.INI aktualisiert wurde. Ist dies der Fall, so lädt der Scanner die neue Version. Der Scanner arbeitet mit Datei-Deltas und Komprimierung, um die Netzwerkbelastung so gering wie möglich zu halten.

Sie sollten die Datei LDAPPL3.INI nicht direkt bearbeiten. Weitere Informationen finden Sie unter "Anpassen und Exportieren der LDAPPL3.INI".

Vorbereitung auf das Konfigurieren

Bevor Sie Produkte konfigurieren, sollten Sie sicherstellen, dass einige (am besten die meisten) Ihrer Clients einen Inventarscan zurückgegeben haben. Standardmäßig gibt der Inventarscanner Anwendungsinformationen für alle ausführbaren Dateien auf jedem einzelnen Client zurück (eine MODE=ALL-Überprüfung). Erst wenn Ihre Clients Inventarscans zurückgegeben haben, enthält die LDAPPL3.INI eine vollständige Liste der auf Ihren Clients installierten Dateien. Sie können eine Datei erst überwachen, wenn diese in der LDAPPL3.INI enthalten ist.

Der erste MODE=ALL-Inventarscan kann eine Größe von mehreren MB haben. Nach dem ersten Scan schickt der Inventarscanner nur noch Deltas, sodass die nachfolgende Scandateien bedeutend kleiner sind. Weitere Informationen zur Verwendung anderer Überprüfungsmodi finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE".

Informationen zu mobilen Clients

Bei mobilen Clients, die vom Netzwerk getrennt sind, erfasst der Softwarelizenzüberwachungsagent weiterhin Daten und speichert diese in der Systemregistrierung des Clients. Sobald der Client wieder eine Netzwerkverbindung hergestellt hat, wird bei der nächsten Überprüfung erkannt, welche der zwischengespeicherten Daten überwacht werden, und diese Daten werden an den Core Server gesendet.

Softwarelizenzüberwachung (Fenster)

Die Fenster für die Softwarelizenzüberwachung sollen es Ihnen ermöglichen, die auf den Clients installierte Software zu überwachen und zu verwalten. Steuern Sie diese Bildschirme vom linken Navigationsfenster aus. Von dort aus können Sie folgende Haupt-Tasks in der Strukturansicht ""Softwarelizenzüberwachung" ausführen.

- **Erfüllung:** In dieser Strukturansicht können Sie die Verwendung und Einhaltung der Lizenzbestimmungen von Produkten innerhalb Ihrer Organisation überwachen, die Herabstufung von Produktlizenzen konfigurieren, Clients die Verwendung von Anwendungen verweigern und Trends hinsichtlich der Erfüllung von Lizenzbestimmungen, der Verwendung und der Verweigerung von Anwendungen betrachten.
- **Aliase:** In dieser Ansicht können Sie Aliasnamen für Produkte oder Lieferanten definieren. Ein Alias gewährleistet, dass Sie auch dann über alle installierten ausführbaren Dateien eines bestimmten Lieferanten oder über ein Produkt genau Buch führen können, wenn sich der Lieferantenname ändert bzw. wenn sich der Lieferant oder der Name des Produkts ändert. Diese Funktion ist insbesondere dann hilfreich, wenn Sie in der Strukturansicht "Erfüllung" Produkte überwachen und genaue Daten zu den Lizenzen verwalten müssen.

Erstellen von Produkt- und Lieferantenaliasnamen

Sie benutzen die Seite "Aliase" zum Erstellen von Produkt- oder Lieferantenaliasnamen. Ein Alias gewährleistet, dass Sie anhand folgender Daten über alle installierten Produkte korrekt Buch führen können:

- **Normalisierung der Daten zu ausführbaren Dateien:** Ein Alias trägt zur Konsistenz der Informationen bei, die zur korrekten Identifizierung eines Produkts von der Core-Datenbank benötigt werden. Beispielsweise sind die von einem Lieferanten bereitgestellten Dateiinformationen nicht immer konsistent. Wenn Dateien verschiedener Microsoft-Produkte in die Core-Datenbank eingelesen werden, kann der Lieferantenname möglicherweise Microsoft Corp, Microsoft (R) oder nur Microsoft lauten. Falls Sie dann eine Abfrage nach Produkten von "Microsoft (R)" ausführen, erhalten eine Liste, die lediglich einen Teil der in Ihrem Netzwerk installierten Microsoft-Produkte umfasst. Durch die Erstellung eines Lieferantenalias namens "Microsoft Corp" für alle in Ihrem Netzwerk installierten Microsoft-Produkte gewährleisten Sie, dass alle diese Produkte über denselben Lieferantennamen verfügen.

- **Aktualisierung der Daten zu ausführbaren Dateien:** Ein Alias ermöglicht es Ihnen, Dateiinformationen zu aktualisieren, falls sich der Produktname oder der Lieferant nach der Installation ändert. Beispielsweise ändern sich gelegentlich Lieferanten- oder Produktnamen, weil eine Firma übernommen oder veräußert wurde oder weil eine Firma ein Produkt nach einigen Versionen umbenannt hat. Wenn dieser Fall bei einer Ihrer Clientanwendungen eintritt, können Sie mithilfe von Aliasnamen die neuen Lieferanten- oder Produktnamen den ursprünglichen Namen zuordnen und damit sicherstellen, dass die Core-Datenbank die ausführbaren Dateien weiterhin korrekt identifizieren kann. Diese Funktion ist insbesondere dann hilfreich, wenn Sie in der Strukturansicht "Erfüllung" Produkte überwachen und genaue Daten zu den Lizenzen verwalten müssen.

Informationen zur Seite "Aliase"

Auf der Seite "Aliase" werden der ursprüngliche Lieferanten- und Produktname sowie die von Ihnen hinzugefügten neuen Lieferanten- und/oder Produktnamen angezeigt. Es muss ein Softwarescan ausgeführt werden, bevor ein neuer Alias in der Strukturansicht "Erfüllung" oder in Berichten angezeigt wird, die Daten zu der auf den Clients installierten Software enthalten.

Sie können zwei verschiedene Alias-Typen erstellen:

- **Lieferant:** Ein Alias für alle installierten Produkte eines bestimmten Lieferanten (geben Sie den ursprünglichen Lieferantennamen und einen neuen Lieferantennamen ein).
- **Produkt:** Ein Alias für ein bestimmtes Produkt (geben Sie die ursprünglichen Lieferanten- und Produktnamen sowie neue Namen ein). Ein Produktalias, der einen neuen Lieferanten enthält, hat stets Vorrang vor einem Alias, der für sämtliche Produkte eines bestimmten Lieferanten definiert wurde.

So definieren Sie einen Alias

1. Klicken Sie im linken Navigationsfenster auf **Software überwachen > Aliase**.
2. Geben Sie den ursprünglichen Lieferantennamen und den ursprünglichen Produktnamen sowie den neuen Lieferanten- und/oder neuen Produktnamen für die Anwendung ein. Sie müssen für alle Aliasfelder Informationen eingeben, selbst wenn die ursprünglichen und neuen Werte identisch sind. Klicken Sie auf **OK**.

Sie können einen Alias bearbeiten und löschen, indem Sie ihn auswählen und auf die Schaltfläche **Alias bearbeiten** oder **Alias löschen** klicken. Nachdem Sie einen Alias gelöscht haben, werden nach dem nächsten Softwarescan wieder der ursprüngliche Lieferanten- und Produktname in der Core-Datenbank verwendet.

Überwachung von Produkten hinsichtlich der Einhaltung von Lizenzbestimmungen

Einrichten eines Produkts

Richten Sie im linken Fensterausschnitt unter "Erfüllung" eine hierarchische Strukturansicht der Produktgruppen und einzelnen Produkte ein. Sie können Produkte beliebig gruppieren, zum Beispiel:

- Nach Firmennamen, wie z. B. Adobe oder Microsoft
- Nach bestimmten Kategorien, wie z. B. "Nicht autorisierte Dateien" oder "Buchhaltungsabteilung"
- Nach Produktsuite, wie z. B. Microsoft Office

In diese Gruppen fügen Sie die Produkte ein, deren Verwendung oder verweigerte Verwendung überwacht werden soll. Sie können beispielsweise der Gruppe "Adobe" Produkte wie Photoshop* und Illustrator* hinzufügen.

Während der Installation werden standardmäßig diese Produktgruppen erstellt, um Ihnen den Einstieg zu erleichtern:

- **LANDesk Management Suite 7.0:** Diese Gruppe enthält Produkt- und Dateicontainer für Management Suite 7.0. Sie müssen lediglich Ihre Lizenzinformationen eingeben, damit die Erfüllung der Lizenzbestimmungen von Management Suite 7.0 auf den Clients überwacht wird.
- **LANDesk Management Suite 8:** Diese Gruppe enthält Produkt- und Dateicontainer für Management Suite 8. Sie müssen lediglich Ihre Lizenzinformationen eingeben, damit die Einhaltung der Lizenzbestimmungen von Management Suite 8 auf Ihren Clients überwacht wird.
- **Microsoft Office:** Diese Gruppe enthält Produkt- und Dateicontainer für Office* 2000 Premium und Office XP Professional. Sie müssen lediglich Ihre Lizenzinformationen eingeben, damit die Einhaltung der Lizenzbestimmungen von Microsoft Office auf Ihren Clients überwacht wird.

So richten Sie ein Produkt ein

1. Klicken Sie im linken Navigationsfenster auf **Software überwachen > Erfüllung**.
2. Wenn Sie keine vorhandene Produktgruppe verwenden möchten, erstellen Sie eine wie unter "Verwalten von Produktgruppen" beschrieben.
3. Klicken Sie auf die Gruppe, in der Sie das Produkt erstellen möchten. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neues Produkt**.
4. Geben Sie die Produktinformationen wie unter "Verwalten von Produkten" beschrieben ein.
5. Setzen Sie die Produktkonfiguration fort, indem Sie die unter "Auswahl zu überwachender Produktdateien" beschriebenen Schritte ausführen.
6. Fügen Sie Lizenzinformationen hinzu, indem Sie die unter "Hinzufügen der Produktlizenzdaten" beschriebenen Schritte ausführen.
7. Exportieren Sie die LDAPPL3.INI, indem Sie die unter "Anpassen und Exportieren der LDAPPL3.INI" beschriebenen Schritte ausführen.

Auswählen der zu überwachenden Produktdateien

Verwenden Sie das Fenster "Dateien zum Produkt hinzufügen" (unter einem Produkt auf die Strukturansicht "Dateien" klicken), um festzulegen, welche Dateien überwacht werden sollen und um auf diese Weise zu erfahren, welche Produkte ausgeführt werden. Wenn Sie im Dialogfeld "Produkteigenschaften" die Option **Alle Dateien abgleichen** ausgewählt haben, müssen sich alle Dateien, die Sie auswählen, auf dem Client befinden, damit die Softwarelizenzüberwachung eine Übereinstimmung registrieren kann. Wenn Sie die Option **Alle Dateien abgleichen** nicht auswählen, wird jegliches Vorhandensein einer Datei in der Liste auf einem Client als Produktübereinstimmung gewertet.

Wenn Sie unterschiedliche Produkte verfolgen, die dieselbe Datei verwenden, müssen Sie die Produkte, die dieselbe Datei verwenden, unterschiedlich behandeln. Beispiel: Wenn Sie die Lizenzverwendung für MSDE und SQL 2000 überwachen und beide Produkte eine Datei SQLSERVR.EXE derselben Größe verwenden, sollten Sie auch eine .DLL oder eine andere Anwendungsdatei überwachen, die jedem dieser Produkte eigen ist. Diese anderen Dateien werden von der Webkonsole nicht hinsichtlich der Einhaltung der Lizenzbestimmungen überwacht (dies geschieht nur bei ausführbaren Dateien); sie erleichtern es dem Scanner lediglich, die MSDE-Lizenz von der SQL 2000-Lizenz zu unterscheiden.

Hinweis: Wenn Sie Dateien, die keine .EXE-Dateien sind, einem Produkt hinzufügen, müssen Sie zuerst die Datei LDAPPL3.TEMPLATE bearbeiten, damit diese bei Softwarescans berücksichtigt werden. Speziell auf die Scanner-Inventarparameter bezogene Informationen sind in der Datei LDAPPL3.TEMPLATE enthalten. Diese Vorlagendatei erkennt zusammen mit der Datei LDAPPL3.INI das Softwareinventar eines Clients. Per Voreinstellung berücksichtigt LDAPPL3.INI nur ausführbare Dateien. Weitere Informationen finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE".

So wählen Sie zu überwachende Dateien aus

1. Geben Sie in das Feld "Suchen" eine Suchzeichenfolge ein. Sie müssen nicht den vollständigen Dateinamen eingeben. Platzhalterzeichen werden nicht unterstützt.
2. Wählen Sie die Inventarspalte aus, die Sie durchsuchen möchten; Lieferant, Produktname, Dateiname, Version und Größe stehen zur Auswahl.
3. Wählen Sie die Dateiliste aus, die Sie durchsuchen möchten; wählen Sie entweder "Alle", "Erkannt" oder "Nicht in Produkt".
4. Durch Klicken auf die Suchschaltfläche neben der Liste **In Spalte** wird die Suche gestartet. Je nachdem, wie viele Übereinstimmungen vorhanden sind, kann es eine Weile dauern, bis die Ergebnisse angezeigt werden.
5. Aktivieren Sie neben Dateien, die die Präsenz dieses Produkts auf Clients signalisieren, das Kontrollkästchen.
6. Wenn Sie angeben möchten, dass eine Datei nicht auf einem Client sein darf, um eine Übereinstimmung mit diesem Produkt zu erzielen, aktivieren Sie das Kontrollkästchen **Aus dem Produkt ausschließen** der betreffenden Datei. Die Kontrollkästchen **Aus dem Produkt ausschließen** befinden sich in der letzten Spalte. Weitere Informationen finden Sie unter "Überwachen von Lizenzen mithilfe der Option "Alle Dateien abgleichen"."

Sie können auch nach Dateien in diesen Dateilisten suchen.

- **Alle:** Alle vordefinierten Dateien in LDAPPL3.INI (selbst wenn sie nicht auf Clients erkannt wurden) und alle Dateien, die auf Clients erkannt wurden.
- **Erkannt:** Nur Dateien, die auf Clients erkannt wurden, auch wenn sie zu Produkten gehören, die in der Datei LDAPPL3 nicht definiert sind.
- **Nicht in Produkt:** Alle Dateien, die zurzeit nicht in der Strukturansicht "Erfüllung" überwacht werden. Mit dieser Liste können Sie nach Dateien suchen, die möglicherweise hinsichtlich der Einhaltung von Lizenzbestimmungen und Trends zur Verwendung/Verweigerung überwacht werden sollten. Diese Ansicht schließt keine Dateien ein, die in der Liste "Verweigert" geführt werden.

Standardmäßig zeigt das Fenster "Dateien" Informationen zu ca. 10 Produkten gleichzeitig an. Sie können die Liste mithilfe der Bildlaufleiste abrollen. Wenn Sie das Fenster länger oder breiter machen möchten, um mehr Dateiinformationen sichtbar zu machen, klicken Sie auf die Schaltfläche für die Größenänderung. Diese Schaltfläche schaltet zwischen kleineren und größeren Ansichten hin und her.

Überwachen von Lizenzen mithilfe der Option "Alle Dateien abgleichen"

Jegliche Datei, die in der Dateiliste eines Produkts enthalten und auf einem Client präsent ist, wird von der Softwarelizenzüberwachung normalerweise als Produktübereinstimmung gewertet. Gelegentlich kann es vorkommen, dass Sie Lizenzen von zwei oder mehr Produkten überwachen müssen, deren ausführbare Dateien denselben Namen und dieselbe Größe haben. In einem solchen Fall müssen Sie zusätzlich eine Datei überwachen, die in den einzelnen Produkten eindeutig ist. Durch Auswahl der Option "Alle Dateien abgleichen" im Dialogfeld "Produkteigenschaften" und den Einsatz der ausführbaren Datei sowie einer eindeutigen Datei zum Erkennen einer Lizenznutzung legen Sie fest, dass alle zu dem Produkt gehörigen Dateien (die sich in dessen Container "Dateien" befinden) auf einem Client installiert sein müssen, bevor die Produktlizenz als genutzt gilt. Damit wird sichergestellt, dass der Scanner die Produktlizenzen korrekt nachverfolgen kann.

Anhand der folgenden beiden Beispiele wird erläutert, wann Sie die Option "Alle Dateien abgleichen" verwenden:

- Wenn Sie die Lizenzverwendung für MSDE und SQL 2000 überwachen und beide Produkte eine Datei SQLSERVR.EXE derselben Größe verwenden, sollten Sie auch eine .DLL oder eine andere Anwendungsdatei überwachen, die jedem dieser Produkte eigen ist. Diese anderen Dateien werden von der Webkonsole nicht hinsichtlich der Einhaltung der Lizenzbestimmungen überwacht (dies geschieht nur bei ausführbaren Dateien); sie erleichtern es dem Scanner lediglich, die MSDE-Lizenz von der SQL 2000-Lizenz zu unterscheiden.
  Hinweis: Wenn Sie Dateien, die keine .EXE-Dateien sind, einem Produkt hinzufügen (um die Option "Alle Dateien abgleichen" verwenden zu können), müssen Sie zuerst die Datei LDAPPL3.TEMPLATE bearbeiten, damit diese bei Softwarescans berücksichtigt werden. Per Voreinstellung berücksichtigt LDAPPL3 nur ausführbare Dateien. Weitere Informationen finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE".

- Wenn Sie 10 Lizenzen für Office XP Standard (enthält Word, Excel, Outlook und PowerPoint) sowie 10 Lizenzen für Office XP Pro (enthält dieselben Anwendungen plus Access) überwachen, stellt sich Ihnen das Problem, dass Sie zwei verschiedene Produktlizenzen überwachen möchten, die gleichnamige und gleich große ausführbare Dateien umfassen. Der Scanner kann Lizenztypen weder anhand einzelner Dateien noch durch den Einsatz der Option "Alle Dateien abgleichen" bei beiden Produkten unterscheiden.

  Sie müssen in diesem Fall einen Schritt weiter gehen und eine ausführbare Datei von Office XP Pro dem Container "Dateien" von XP Standard hinzufügen und diese ausführbare Datei durch Auswahl von **Aus dem Produkt ausschließen** als nicht zum Produkt gehörig markieren. Damit wird sichergestellt, dass der Softwarelizenzüberwachungsagent keine Office XP Pro-Lizenz als XP Standard-Lizenz verzeichnet, was der Fall wäre, wenn lediglich die Option "Alle Dateien abgleichen" ausgewählt würde. Weitere Informationen zum Kennzeichnen einer Datei als ausgeschlossene Datei finden Sie unter "Auswahl der zu überwachenden Produktdateien".

Hinzufügen der Produktlizenzdaten

Sie müssen Lizenzinformationen hinzufügen, damit die Einhaltung der Lizenzbestimmungen für ein Produkt überwacht werden kann. Falls Sie lediglich die Produktverwendung nachverfolgen möchten, können Sie diesen Schritt übergehen.

Nachdem Sie die Lizenzinformationen für ein Produkt angegeben haben, wird durch ein rotes Symbol mit einem Ausrufezeichen neben einer Produktgruppe angezeigt, dass ein Produkt dieser Gruppe nicht den Lizenzbedingungen entsprechend verwendet wird. Erweitern Sie die Produktgruppe, um das betreffende Produkt ausfindig zu machen, und betrachten Sie die zugehörigen Informationen im rechten Fensterausschnitt.

So fügen Sie Produktlizenzdaten hinzu

1. Klicken Sie auf **Software überwachen > Erfüllung >** ***Produktgruppe*** **>** ***Produktname***.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Lizenz**.
3. Geben Sie auf den Registerkarten des Dialogfelds "Lizenzeigenschaften" die Informationen zu Lizenz, Kauf und Verfolgung ein, die für Ihre Organisation relevant sind.
4. Nach der Eingabe aller erforderlichen Daten klicken Sie auf **OK**.
5. Wenn Sie sicherstellen möchten, dass alle zu einem Produkt gehörigen ausführbaren Dateien auf einem Client installiert sind, bevor die Einhaltung der Lizenzbestimmungen für das betreffende Produkt überwacht wird, können Sie im linken Fensterausschnitt mit der rechten Maustaste auf den Produktnamen klicken und die Option **Alle Dateien abgleichen** wählen. Weitere Informationen finden Sie unter "Überwachen von Lizenzen mithilfe der Option "Alle Dateien abgleichen"."

Informationen zum Dialogfeld "Lizenzeigenschaften"

Das Dialogfeld "Lizenzeigenschaften" besitzt drei Registerkarten:

- Lizenz
- Kaufdaten
- Verfolgung

Auf der Registerkarte "Lizenz" konfigurieren Sie die Lizenzeigenschaften des Produkts.

- **Lizenznummer:** Geben Sie hier eine gültige Lizenznummer für das Produkt ein.
- **Lizenztyp:** Geben Sie den Typ der Lizenz an, die Sie für das Produkt besitzen, z. B.: Kostengünstiges Upgrade, Freeware, Neuerwerb, OEM, Produktupgrade, Public Domain, Shareware, unbekannt.
- **Anzahl:** Geben Sie die Anzahl der von Ihnen erworbenen Produktlizenzen ein.
- **Seriennummer:** Geben Sie hier eine zusätzliche Nummer ein, die zur Produktlizenz gehört.

Auf der Registerkarte "Kaufdaten" konfigurieren Sie die Kaufmerkmale der Produktlizenz.

- **Kaufdatum:** Geben Sie das Datum ein, an dem das Produkt von Ihrem Unternehmen gekauft wurde.
- **Stückpreis:** Geben Sie den Preis jeder für dieses Produkt erworbenen Lizenz ein.
- **Bestellnummer:** Geben Sie die für den Kauf verwendete Bestellnummer ein.
- **Wiederverkäufer:** Geben Sie den Namen des Händlers ein.

Auf der Registerkarte "Verfolgen" konfigurieren Sie die Eigenschaften des Produkts, die zur Nachverfolgung dienen.

- **Eigentümer:** Geben Sie die Person oder Abteilung Ihrer Firma ein, die für die Aufbewahrung des verpackten Produkts verantwortlich ist.
- **Ort:** Geben Sie den Ablageort an, an dem das verpackte Produkt aufbewahrt wird.
- **Notizen:** Geben Sie zusätzliche Informationen zur Produktlizenz ein, z. B. Möglichkeiten der Lizenzherabstufung.

Anpassen und Exportieren der LDAPPL3.INI

Der Client-Inventarscanner verwendet eine Textdatei mit dem Namen LDAPPL3.INI. Diese Datei enthält Informationen zum Softwareinventar. Die LDAPPL3.INI wird anfänglich mit den am häufigsten verwendeten Dateinamen von Anwendungsprogrammdateien und Dateiinformationen gefüllt. Wenn der Scanner auf Clients ausgeführt wird, verwendet er eine lokale LDAPPL3.INI-Kopie, um Dateinamen von ausführbaren Clientdateien mit den Softwareinventardaten abzugleichen.

Die Master-LDAPPL3.INI befindet sich in der LDLogon-Freigabe des Core Servers. Jedes Mal, wenn Sie eine Änderung in den Softwarelizenzüberwachungsdaten vornehmen, müssen Sie eine neue LDAPPL3.INI-Datei exportieren.

So exportieren Sie eine neue LDAPPL3.INI

1. Klicken Sie im linken Navigationsfenster auf **Software überwachen | Erfüllung**.
2. Klicken Sie in einem Softwarelizenzüberwachungsfenster auf **Liste veröffentlichen**.
3. Klicken Sie auf der Seite "Liste veröffentlichen" auf **Weiter**.

Von Ihnen vorgenommene Änderungen werden auf den Clients erst dann wirksam, nachdem die Clients die aktualisierte LDAPPL3.INI erhalten haben.

Beim Exportieren einer neuen LDAPPL3.INI erstellt der Core Server mithilfe der LDAPPL3.TEMPLATE-Textdatei der LDLogon-Freigabe das Framework für die exportierte LDAPPL3.INI. Der Core Server füllt dieses Framework dann mit Dateiinformationen und Softwarelizenzüberwachungsdaten aus der Core-Datenbank. Zuletzt schreibt der Core Server die exportierte LDAPPL3.INI-Datei in die LDLogon-Freigabe und ersetzt dabei alle etwaigen vorhandenen Versionen. Wenn die Clients das nächste Mal einen Softwarescan ausführen, erhalten sie automatisch die aktualisierte LDAPPL3.INI.

Sie sollten die LDAPPL3.INI nicht direkt in einem Texteditor bearbeiten, da die Daten in der Core-Datenbank des Core Servers gespeichert werden. Wenn der Server eine neue Version dieser Datei schreibt, gehen Änderungen, die Sie direkt mit einem Editor vorgenommen haben, verloren. Alle Änderungen an der LDAPPL3.INI sollten in der LDAPPL3.TEMPLATE-Datei im Fenster für die Verfolgung der Softwarelizenzerfüllung von der Webkonsole aus vorgenommen werden.

Erläuterungen zu den Inventardatei-Überprüfungsmodi

Wenn der Inventarscanner auf eine Datei trifft, die nicht in der LDAPPL3.INI definiert ist, bestimmt der Scanner, welche Dateiinformationen er verwenden kann und leitet die neuen Dateiinformationen an den Core Server weiter. Dies ist die Standardprüfmethode (MODE=ALL scanning). Da Sie nur Softwarelizenzen für Dateien überwachen können, die in der Datenbank auf dem Core Server definiert sind, können Sie mit der Durchführung einer MODE=ALL-Prüfung die Datenbank mit Dateien auf Ihren Clients auf dem neusten Stand halten.

Wenn Sie die Softwarelizenzüberwachung nicht einsetzen oder nur an der Überprüfung von Anwendungen interessiert sind, die in der LDAPPL3.INI definiert sind, können Sie eine MODE=LISTED-Prüfung verwenden, um den Prüfaufwand zu reduzieren. Bei dieser Überprüfung werden nicht-definierte Dateien ignoriert. Weitere Informationen zur Verwendung anderer Überprüfungsmodi finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE".

Standardmäßig enthält LDAPPL3.INI nur Beschreibungen ausführbarer Dateien. Falls der Scanner auch andere Typen von Anwendungsdateien (.DLL-, .COM-, .SYS-Dateien usw.) erkennen soll, können Sie die LDAPPL3.TEMPLATE-Datei so bearbeiten, dass alle Dateien dieses Typs bei einer Überprüfung berücksichtigt werden. Weitere Informationen finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE".

So stellen Sie die LDAPPL3.INI-Datei Clients zur Verfügung

Jeder Client, der den Inventarscanner ausführt, besitzt eine lokale Kopie der LDAPPL3.INI. Die Datei LDAPPL3.INI der Clients wird anfänglich im Rahmen des Standard-Client-Konfigurationssetup installiert. Die Client- und die Core-Version dieser Datei müssen synchronisiert werden, damit der Scanner weiß, welche Dateien auf den Clients zu überprüfen oder zu verweigern sind. Die Core Server- und Client-LDAPPL3.INI-Sychronisierung erfolgt mittels Delta-Matching, sodass nur die Änderungen weitergeleitet werden. Mithilfe der Dateikomprimierung wird die LDAPPL3.INI des Core Servers um weitere 70 Prozent komprimiert, wodurch der Scanner die entsprechende LDAPPL3.INI der Clients aktualisieren kann, ohne nennenswerte Bandbreite zu beanspruchen.

Wenn Sie nicht abwarten möchten, bis die Datei LDAPPL3.INI durch den nächsten Inventarscan auf den Clients aktualisiert wird, können Sie die Änderungen den Clients zur Verfügung stellen, indem Sie einen Auftrag planen, der die LDAPPL3.INI pushbasiert auf die Clients überträgt.

Betrachten von Trends hinsichtlich der Einhaltung von Lizenzbestimmungen sowie der Verwendung und Verweigerung von Produkten

IT Management Suite beinhaltet umfassende Berichtfunktionen für die Softwarelizenzüberwachung. Sie können diese Berichte anzeigen, indem Sie **Inventar> Berichte** aufrufen und auf **Softwarelizenzierung** klicken.

Die Softwarelizenzüberwachungsberichte stellen u.a. folgende Informationen zur Verfügung:

- Anwendungsverwendung pro Computer
- Anwendungen, die nicht eine bestimmte Anzahl von Malen verwendet wurden (nützlich für die Identifizierung ungenutzter Lizenzen)
- Ausführungsversuche mit verweigerten Produkten und damit verknüpfte Benutzer
- Lizenznutzung nach Computer und Produkt

Verweigern der Produktausführung

Sie können Clients an der Ausführung bestimmter Dateien, die von Ihnen angegeben werden, hindern. Wenn Sie ein Produkt hinzufügen oder die Eigenschaften eines Produkts bearbeiten, können Sie die Option **Verweigertes Produkt** aktivieren. Wenn Clients versuchen, ein verweigertes Produkt auszuführen, lässt sich das Produkt auf ihrem System nicht starten und es wird eine Meldung angezeigt, in der mitgeteilt wird, dass der zuständige Systemadministrator den Zugriff auf das betreffende Programm gesperrt hat. Sie können den normalen Zugriff auf ein Produkt wiederherstellen, indem Sie die Option **Verweigertes Produkt** deaktivieren.

Alle Dateien in der Dateiliste eines verweigerten Produkts werden auf den Clients verweigert. Die Produktoption **Alle Dateien abgleichen** wirkt sich nicht auf verweigerte Produkte aus.

Sie müssen die LDAPPL3.INI veröffentlichen und Clients müssen die aktualisierte Version erhalten, bevor etwaige Änderungen wirksam werden.

Verteilen von Software und Dateien

Einrichten eines Delivery-Servers für Verteilungspakete

Der Delivery-Server ist der Webserver, auf dem Pakete gespeichert werden, die Sie verteilen möchten. In den folgenden Schritten wird beschrieben, wie ein virtuelles Verzeichnis auf einem Webserver erstellt und für Suchvorgänge aktiviert wird. Im Allgemeinen gilt, dass sich virtuelle Verzeichnisse lesen und durchsuchen lassen müssen. Die Berechtigung zum Ausführen lässt sich nicht aktivieren, da andernfalls die Freigabe nicht korrekt funktioniert. Außerdem sollten Sie Schreibberechtigungen deaktivieren, damit Clients den Ordnerinhalt nicht ändern können.

So konfigurieren Sie einen Windows NT/2000-Webserver für die Softwareverteilung

1. Erstellen Sie einen Ordner auf dem Webserver, in dem die Softwareverteilungspakete gespeichert werden sollen. Im Normalfall wird dafür auf einem IIS-Webserver ein Unterordner des Ordners c:\inetpub\wwwroot verwendet.
2. Kopieren Sie die Pakete in diesen Ordner.
3. Doppelklicken Sie in der Systemsteuerung auf **Verwaltung** und anschließend auf **Internetdienste-Manager**.
4. Doppelklicken Sie im rechten Bereich auf das Symbol mit dem Namen des Clients, und klicken Sie auf **Standardwebsite**.
5. Klicken Sie im rechten Bereich mit der rechten Maustaste auf eine freie Stelle, wählen Sie **Neu**, und klicken Sie auf **Virtuelles Verzeichnis**.
6. Klicken Sie im Assistenten auf **Weiter**, und geben Sie einen Alias für den Ordner ein. Klicken Sie auf **Weiter**.
7. Geben Sie den Pfad ein, oder wechseln Sie zum gewünschten Pfad, und klicken Sie auf **Weiter**.
8. Aktivieren Sie im Dialogfeld "Zugriffsberechtigungen" die Optionen **Skript ausführen** und **Durchsuchen**. So können Sie Pakete beim Erstellen des Softwareverteilungsskripts durchsuchen. Klicken Sie auf **Weiter** und auf **Fertig stellen**.
9. Um **Port 80** auf dem Webserver zu aktivieren, klicken Sie im linken Bereich mit der rechten Maustaste auf **Standardwebsite**.
10. Klicken Sie auf **Eigenschaften**. Im Dialogfeld "Identifikation der Webseite" muss im Feld "TCP-Port" der Wert 80 angezeigt werden. Andernfalls müssen Sie auf **Erweitert** klicken, um den Port hinzuzufügen.
11. Stellen Sie sicher, dass die Website verfügbar ist, indem Sie einen Browser öffnen und den URL des Webservers sowie ein virtuelles Verzeichnis eingeben. Wenn der Webserver "Test" heißt und der Name des virtuellen Verzeichnisses "Pakete" lautet, geben Sie folgenden URL ein:

    ```
    http://Test/Pakete
    ```

    Eine Liste der Pakete, die in diesen Ordner kopiert wurden, wird angezeigt.

Sofern der Speicherplatz der Festplatte dies zulässt, können Sie Pakete in beliebiger Größe und Anzahl in diesem Ordner speichern. Zur logischen Gruppierung von Paketen können Sie Unterordner verwenden. Für jeden Unterordner, den Sie erstellen, müssen Sie die oben beschriebenen Zugriffsberechtigungen festgelegt haben.

Sobald Sie die Pakete auf eine Paketfreigabe eines Webservers kopiert haben, werden sie bereitgestellt und können auf die Zielclients kopiert werden. Wenn das Paket an der Reihe ist, wird sein URL oder UNC-Pfad als Befehlszeilenparameter an SDCLIENT.EXE (den Clientagent) übergeben. SDCLIENT.EXE verwaltet die Dateiübertragung, startet die Installation und erstellt Statusberichte.

Der Webserver kommuniziert mit dem Client, um sicherzustellen, dass das Paket richtig kopiert wird. Wenn die Paketübertragung beim Download unterbrochen wird, kann der Webserver den Download mithilfe des HTTP-Protokolls an der Stelle fortsetzen, an der er unterbrochen wurde.

Zusätzliche Windows Server 2003-Webkonfiguration für die Softwareverteilung

Windows Server 2003 behandelt virtuelle Verzeichnisse anders als Windows 2000. Wenn Sie auf einem Windows Server 2003 ein Verzeichnis auswählen und es über das Kontextmenü als Webfreigabe festlegen, registriert sich das Verzeichnis in IIS 6 selbst als Webanwendung statt als virtuelles Verzeichnis. Problematisch an der Registrierung als Webanwendung ist hierbei, dass der Webserver bei der Auswahl einer ausführbaren Datei versucht, die Datei als Webanwendung auszuführen statt sie zum Benutzer herunterzuladen. Die Lösung besteht darin, das freigegebene Verzeichnis im IIS von einer Webanwendung in ein virtuelles Verzeichnis zu ändern und die Berechtigungen zum Ausführen zu deaktivieren..

Auf Windows 2003-Webservern müssen Sie zudem die anonyme Authentifizierung für den Paketordner aktivieren.

So aktivieren Sie die anonyme Authentifizierung

1. Klicken Sie auf **Start | Verwaltung | Internetinformationsdienste-Manager**.
2. Klicken Sie auf **Lokaler Computer > Websites > Standardwebsite >** Ihr Paketverzeichnis.
3. Klicken Sie im Kontextmenü Ihres Paketverzeichnisses auf **Eigenschaften**. Klicken Sie auf der Registerkarte **Sicherheit** für **Authentifizierung und Zugriffskontrolle** auf **Bearbeiten** und aktivieren Sie das Kontrollkästchen **Anonymen Zugriff aktivieren** im Fenster **Authentifizierungsmethoden**.

Planen und Verteilen von Softwarepaketen

Mit der Webkonsole können Sie folgende Softwaredistributionstasks ausführen:

- Softwarepakete planen und an die Clients verteilen
- Geplante Aufträge anzeigen
- Verteilungsskripts anzeigen
- Verteilungsprotokolle anzeigen

Der Vorteil der Webkonsole gegenüber der Management Suite-Konsole besteht darin, dass Sie Pakete an Clients in einer Rollup-Datenbank verteilen können. Das bedeutet, dass Sie ein Paket an mehrere tausend Clients gleichzeitig senden können.

Sie können mit der Webkonsole nur Pakete planen und installieren; die Pakete selbst müssen von Ihnen auf einem festzugeordneten Computer mithilfe des Package Builder erstellt werden. Bevor Sie die Webkonsole zum Planen und Installieren von Paketen verwenden, müssen Sie mithilfe von Package Builder ein Paket erstellen und auf Ihrem Webserver speichern. Weitere Informationen finden Sie unter "Einrichten eines Paketerstellungscomputers" und "Einrichten des Übermittlungsservers" in Kapitel 6 des *Benutzerhandbuchs*. Sie können pro Job ein Einzeldatei-Paket verteilen. Idealerweise sollte es sich bei Ihrem Paket um eine selbstextrahierende Einzeldatei und eine selbstinstallierende ausführbare Datei handeln. Wenn die Datei über eine ausführbare Erweiterung verfügt, führt die Softwareverteilung die Datei auf den Clients aus, sobald ihnen die Datei zugestellt wird. Wenn die Datei nicht über eine ausführbare Erweiterung verfügt, wird sie lokal in den Ordner \ldclient\sdmcache des Clients kopiert.

Beachten Sie, dass folgende Verteilungsfunktionen beim einer Softwareverteilung von der Webkonsole aus nicht zur Verfügung stehen:

1. Die Möglichkeit, zusätzliche Dateien für das Multicasting auszuwählen.
2. Peerdownload (nur vom Cache oder Peer installieren).
3. Dynamische Bandbreitendrosselung:
   - Auf Client zu verwendender minimal verfügbarer Bandbreitenprozentsatz
   - Verzögerung zwischen Paketen (Peer)
   - Verzögerung zwischen Paketen (Quelle)
4. Multidatei-MSI-Verteilung mittels Multicast.

Verwenden des Softwareverteilungsassistenten

Sobald Sie ein Paket erstellt haben, können Sie es in fünf Schritten mit dem Softwareverteilungsassistenten planen und vom Web aus verteilen. Der Assistent umfasst folgende Schritte:

1. Einrichten eines Pakets zum Verteilen
2. Auswählen von Clients, die das Paket erhalten sollen
3. Uhrzeit und Datum für den Verteilungsauftrag planen
4. Verteilungsauftragswerte prüfen und Änderungen vornehmen, falls erforderlich
5. Anzeigen der Auftragsergebnisse

So starten Sie den Softwareverteilungsassistenten

1. Klicken Sie im linken Navigationsfenster auf **Software verteilen**.
2. Klicken Sie auf der Seite **Software Distribution** auf **Ein Paket verteilen**.

Die Seite **Software Distribution – Pakete** wird angezeigt. Nun wird der Assistent gestartet, mit dem Sie ein Softwarepaket planen und verteilen können.

Konfigurieren der Softwareverteilung auf Domänenebene und Konfigurieren der Windows 2003-Server

Wenn Sie die Softwareverteilung über die Webkonsole vornehmen möchten, muss der Webserver, auf dem Sie die Webkonsole installiert haben, auf die Softwareverteilungsdateien auf dem Core Server zugreifen und sie ändern können. Dies ist dann ein Thema, wenn sich Webserver und Core Server auf verschiedenen Computern befinden oder wenn auf dem Webserver das Betriebssystem Windows 2003 Server verwendet wird. Hierzu müssen Sie eine Komponente auf dem Webserver registrieren.

So konfigurieren Sie die Domänenebenen-Softwareverteilung

1. Suchen Sie den Webserver auf, auf dem Sie die Webkonsole installiert haben.
2. Doppelklicken Sie in der Windows-Systemsteuerung auf "Verwaltung" und anschließend auf **Komponentendienste**.
3. Klicken Sie auf **Komponentendienste > Computer > Arbeitsplatz > COM+-Anwendungen**.
4. Klicken Sie im Kurzbefehlmenü für **COM+-Anwendungen** auf **Neu | Anwendung**.
5. Klicken Sie auf der Begrüßungsseite des Assistenten auf **Weiter**.
6. Klicken Sie auf **Leere Anwendung erstellen** und auf **Weiter**.
7. Geben Sie einen Namen für die neue Anwendung ein. Beispielsweise "LANDesk". Klicken Sie auf **Serveranwendung** und auf **Weiter**.
8. Klicken Sie auf **Dieser Benutzer**. Sie müssen ein Domänenebenenkonto mit administrativen Rechten auf dem Core Server eingeben. Wenn es sich um kein Konto auf Domänenebene handelt, funktioniert die Softwareverteilung von der Webkonsole nicht. Klicken Sie auf **Weiter**.
9. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen. Es wird ein COM+-Anwendungsstrukturknoten mit dem Namen "LANDesk" oder dem von Ihnen gewählten Namen angezeigt.
10. Klicken Sie auf **Komponentendienste > Computer > Arbeitsplatz > COM+-Anwendungen > LANDesk > Komponenten**.
11. Klicken Sie im Kurzbefehlmenü **Komponenten** auf **Neu | Komponente**.
12. Klicken Sie auf der Begrüßungsseite des Assistenten auf **Weiter**.
13. Klicken Sie auf **Komponente(n) importieren,die bereits registriert sind**.
14. Klicken Sie in der Komponentenliste auf **Schcom.Schint.1** und anschließend auf **Weiter**.
15. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen. Schcom.Schint.1 sollte nun als registrierte Komponente angezeigt werden.
16. Klicken Sie auf **Komponentendienste > Computer > Arbeitsplatz > COM+-Anwendungen > LANDesk > Rollen**.
17. Klicken Sie im Kontextmenü für **Rollen** auf **Neu | Rolle** und geben Sie "Jeder" als Name des neuen Elements ein.
18. Klicken Sie auf **Rollen > Jeder > Benutzer**. Klicken Sie im Kontextmenü für **Benutzer** auf **Neu | Benutzer**, geben Sie "Jeder" als Objektname ein und klicken Sie auf **OK**.
19. Starten Sie IIS erneut oder führen Sie einen Neustart aus.

Verwenden von Targeted Multicast® mit Software Distribution

Die LANDesk Targeted Multicast®-Technologie ermöglicht es, mit einem minimalen Aufkommen an Netzwerkverkehr umfangreiche Pakete über das Netzwerk an viele Benutzer zu verteilen. Targeted Multicast-Funktionen erfordern weder zusätzliche Hardware- oder Software-Infrastruktur noch spezielle Router-Konfigurationen für das Versenden von Multicast-Paketen. Sie erhalten die außerordentlichen Vorteile der Multicast-Technologie ohne die sonst üblichen Probleme.

Targeted Multicast funktioniert mit den vorhandenen Softwareverteilungspaketen. Wenn Sie Targeted Multicast verwenden, ist das Verteilen der Software ganz einfach, selbst in WAN-Umgebungen mit mehreren Hops und niedrigen Verbindungsgeschwindigkeiten (56 KBit/s). Targeted Multicast verwendet HTTP für die Übermittlung von einer Website an einen Subnetzrepräsentanten. Der Management Suite-Inventarscanner stellt dem Targeted Multicast-Dienst alle Subnetzinformationen zur Verfügung.

Targeted Multicast bietet zahlreiche Vorteile, die Standard-Multicast-Methoden nicht aufweisen. Mithilfe der inventarbasierten Angabe von Clients können Sie ein Paket über ein Broadcast an eine ausgewählte Gruppe von Computern, die bestimmte Kriterien erfüllen, senden. Mit Targeted Multicast wird das Verfahren auch deshalb vereinfacht, weil Router nicht extra für die Verarbeitung von übermittelten Paketen konfiguriert werden müssen.

Verglichen mit konventionellen Softwareverteilungsmethoden wird bei der Übermittlung von Softwarepaketen mit Targeted Multicast deutlich weniger Zeit und Bandbreite benötigt. Statt für jeden Client ein Paket über das Netzwerk zu senden, wird für jedes Subnetz nur eine Übertragung durchgeführt. Je höher die Anzahl der Clients in jedem Subnetz, desto mehr Bandbreite wird eingespart.

Sowohl Windows- als auch Macintosh OS 10.2-Clients unterstützen Targeted Multicast.

Wenn Sie Targeted Multicast aktivieren möchten, wählen Sie die Option **Dieses Paket mit Multicast verteilen** auf der Seite **Software Distribution - Pakete**, die beim Erstellen eines Verteilungspaketskripts angezeigt wird.

Wie Targeted Multicast funktioniert

Die Tageted Multicast-Funktion unterteilt Ihr Netzwerk in Multicast-Domänen. Jede Multicast-Domäne besteht aus Clients, von denen jeder den Broadcast-Verkehr des anderen Clients hören kann. Router blockieren normalerweise Multicast-Daten, sodass eine Multicast-Domäne oft einem Subnetz in Ihrem Netzwerk entspricht. Targeted Multicast erkennt diese Multicast-Domänen automatisch, wenn Sie einen Auftrag für die Verteilung mit Multicast planen. Sie brauchen keine Änderungen an Ihren Netzwerkkonfiguration vorzunehmen, um ein fehlerfreies Arbeiten des Targeted Multicast zu gewährleisten.

Jede Multicast-Domäne erfordert einen Multicast-Domänenrepräsentanten. Ein Repräsentant ist der Client in einer Multicast-Domäne, der die Datei, die an andere Clients in derselben Multicast-Domäne verteilt wird, per Multicasting verteilt. Jeder Client, auf dem der Software Distribution-Agent installiert ist, kann als Multicast-Domänenrepräsentant fungieren. Targeted Multicast wählt Multicast-Domänenrepräsentanten automatisch für jede Multicast-Verteilung aus. Clients, die als Repräsentanten fungieren, benötigen keine zusätzliche Software.

Wenn ein Multicast-Domänenrepräsentant erkannt wird, sucht Targeted Multicast zuerst in jeder Multicast-Domäne nach einem Client, auf dem sich das Paket bereits in dessen Softwareverteilungs-Cache befindet. Clients legen Pakete, die Ihnen per Verteilung zugestellt werden, vor dem Installieren im Cache-Speicher ab. Wenn Targeted Multicast einen Client findet, der das Paket im Cache-Speicher abgelegt hat, setzt Targeted Multicast diesen Client als den Multicast-Domänenrepräsentanten ein. Die Verwendung eines Pakets aus dem Cache-Speicher spart Bandbreite und Zeit, da der Server das Paket nicht zuerst noch an anden Multicast-Domänerepräsentanten senden muss.

Wenn Targeted Multicast keinen Client mit einem Paket im Cache-Speicher findet, sendet es einen Subnetz-Broadcast, um einen Client zu finden, der Multicast-Domänenrepräsentant sein könnte.

Falls mit keiner dieser Multicast-Erkennungsmethoden ein Multicast-Repräsentant gefunden werden kann, kontaktiert der Multicast-Server jeden Client in der Zielliste, um zu ermitteln, ob er Multicast-Repräsentant sein könnte.

Aufgrund der zusätzlichen Schritte, die Targeted Multicast beim Verteilen von Paketen durchläuft, beansprucht die Multicast-Paketverteilung u.U. mehr Zeit als eine normale Paketverteilung. Dies gilt besonders für kleine Pakete oder Verteilungen, die nur auf eine geringe Anzahl von Clients gerichtet sind. Aktivieren Sie die Multicast-Option, wenn Sie (vor allem große) Pakete an viele Clients gleichzeitig verteilen oder wenn der Minimierung des Netzwerkbandbreitenkonsums Beachtung geschenkt werden muss.

Wenn Sie eine Verteilung mithilfe von Targeted Multicast starten, wird das Fenster "Multicast Software Distribution" angezeigt. Dieses Fenster enthält ausführliche Informationen zum Verteilungsvorgang.

Anzeigen der geplanten Aufträge

Sie können jeden mit der Webkonsole geplanten Verteilungsauftrag anzeigen, löschen oder neu planen.

So zeigen Sie geplante Aufträge an

1. Klicken Sie im linken Navigationsfenster auf **Software verteilen**.
2. Klicken Sie auf der Seite "Software Distribution" auf **Geplante Aufträge anzeigen**.

Es wird eine Tabelle angezeigt, in der die zur Verteilung von Paketen geplanten Verteilungsaufträge aufgeführt sind. Die Tabelle enthält folgende Spalten:

- **Kennung:** Die Kennung ist eine fortlaufende, willkürliche Nummer, die jedem geplanten Auftrag zugewiesen wird.
- **Task:** Der Skriptname für einen bestimmten Verteilungsauftrag. Klicken Sie auf einen Namen, um die Clients anzuzeigen, für die der Auftrag geplant wurde. Die Symbole in dieser Spalte bedeuten Folgendes:
  - Der Auftrag wird nur einmal angezeigt.
  - Der Auftrag fällt in regelmäßigen Abständen an.

- **Status:** Zeigt den aktuellen Status des Verteilungsauftrags an. Der Status "Vorgänge teilweise abgeschlossen" bedeutet, dass das Paket an einige Clients erfolgreich verteilt wurde, an andere hingegen nicht. Um festzustellen, welche Clients das Paket installiert haben, klicken Sie auf den Tasknamen und zeigen Sie den Status jedes einzelnen Client an, für den der Auftrag geplant wurde:
- **Letzte Ausführung:** Zeigt den Tag und die Uhrzeit an, für den bzw. die der Auftrag geplant ist.

Klicken Sie auf **Seite aktualisieren**, um die Liste der geplanten Aufträge zu aktualisieren.

Anzeigen der Verteilungsskripts

Sie können einen Auftrag für alle Skripts, die als Pakete verteilt werden, anzeigen, löschen oder neu erstellen. Diese Skripte werden standardmäßig im Ordner "C:\Program Files\LANDesk\ManagementSuite\scripts" auf dem Core Server gespeichert.

So zeigen Sie Verteilungsskripts an

1. Klicken Sie im linken Navigationsfenster auf **Software verteilen**.
2. Klicken Sie auf der Seite "Software Distribution" auf **Verteilungsskripte anzeigen**.

Klicken Sie zum Löschen eines Skripts aus der Liste auf das Skript und anschließend auf **Skript löschen**. Schlägt der Löschvorgang fehl, liegt dies vermutlich an einem anstehenden Auftrag. Löschen Sie vor dem Löschen des Skripts den Auftrag auf der Seite "Software Distribution – Geplante Aufträge".

Klicken Sie zum Anzeigen des Inhalts eines Skripts in der Liste auf das Skript und anschließend auf **Skript anzeigen**. Die Inhalte können Sie nur anzeigen und nicht bearbeiten.

Um einen neuen Auftrag für das Skript zu erstellen, klicken Sie auf das Skript und anschließend auf **Neuen Auftrag erstellen**. Führen Sie dann erneut den Assistenten aus, um verschiedene Auftragseinstellungen für dieses bestimmte Skript zu konfigurieren.

Anzeigen der Verteilungsprotokolle

Sie können Verteilungsprotokolle, die während eines Softwaredistributionsauftrags erstellt wurden, anzeigen oder löschen. Diese Protokolle werden standardmäßig im Ordner "C:\Program Files\LANDesk\ManagementSuite\log" auf dem Core Server gespeichert.

So zeigen Sie Verteilungsprotokolle an

1. Klicken Sie im linken Navigationsfenster auf **Software verteilen**.
2. Klicken Sie auf der Seite **Software Distribution** auf **Verteilungsprotokolle anzeigen**.

Zum Anzeigen oder Löschen eines Protokolls in der Liste wählen Sie das Protokoll, und klicken Sie anschließend auf **Verteilungsprotokoll anzeigen** bzw. **Verteilungsprotokoll löschen**. Wenn Sie soeben ein Paket an Clients verteilt haben und das Protokoll noch nicht in der Liste aufgeführt wird, klicken Sie auf **Seite aktualisieren**.

Anpassen der Webkonsole

Verwenden von Rollup-Datenbanken

Mithilfe des Datenbank-Rollup-Tools (DBROLLUP.EXE) können Sie mehrere Quell-Datenbanken in einer einzigen Ziel-Core-Rollup-Datenbank kombinieren. Eine Core Server-Datenbank kann ca. 10.000 Clients unterstützen. Die Höchstzahl der Rollup-Core-Clients hängt von der Hardware und dem akzeptablen Leistungsgrad ab. Die Quell-Datenbank kann entweder ein Core Server oder ein Rollup-Core Server sein.

Die Systemanforderungen für eine Zieldatenbank können erheblich höher sein als die Systemanforderungen für eine Standarddatenbank. Diese Anforderungen können in Abhängigkeit von der Netzwerkumgebung erheblich variieren. Wenn Sie weitere Informationen über die Hard- und Softwareanforderungen für die Zieldatenbank benötigen, wenden Sie sich an den LANDesk-Software-Support.

Das Setup installiert das Datenbank-Rollup-Tool automatisch mit dem Rollup-Core. Das Rollup-Tool verwendet einen Pull-Mechanismus für den Zugriff auf die von Ihnen ausgewählten Cores. Damit Datenbank-Rollups funktionieren, muss bereits ein Laufwerk zu jedem Core zugeordnet sein, von dem das Rollup-Tool Daten abrufen soll. Das Konto, zu dem Sie eine Verbindung herstellen, muss über Leserechte für die Registrierung des Core Servers verfügen.

Das Rollup-Tool prüft durch einen Registrierungsschlüssel auf dem Core Server die Datenbank- und Verbindungsdaten (HKLM\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\local) und verwendet die Daten dieses Schlüssels, um auf die mit jedem Core verknüpfte Datenbank zuzugreifen, die Sie dem Rollup-Tool hinzugefügt haben. Bei Oracle-Datenbanken muss die TNS-Definition auf dem Server, auf dem Sie das Rollup-Tool ausführen, der TNS-Definition auf dem Core Server entsprechen, auf den das Tool zugreift.

Sie können das Rollup-Tool verwenden, um die Attribute auszuwählen, für die ein Rollup von den Cores durchgeführt werden soll. Die von Ihnen ausgewählten Attribute gelten für alle Cores. Durch Verringern der Attributzahl wird die Rollup-Zeit und die während den Rollups übertragene Datenmenge reduziert. Wenn Sie wissen, dass Sie keine Abfragen nach gewissen Attributen durchführen, können Sie diese entfernen.

Das Rollup-Tool führt stets einen Rollup der ausgewählten Attributdaten und der Softwarelizenzüberwachungs-Daten durch. Sie können Softwarelizenzüberwachungs-Rollups nicht anpassen. Rollups enthalten auch weder Abfragen noch von Ihnen definierten Bereiche. Alle Konsolenbenutzer mit Rechten für die Rollup-Datenbank haben auf alle Daten in dieser Datenbank Zugriff. Sie können die Sicherheit auf Funktionsebene verwenden, um den Zugriff auf Webkonsolenfunktionen einzuschränken. Weitere Informationen finden Sie unter "Einrichten der Sicherheit auf Funktionsebene für Rollup-Datenbanken".

Nachdem Sie die Core Server für den Rollup und die Attributliste für diese Server hinzugefügt haben, können Sie auf **Planen** klicken, um das Skript für einen geplanten Rollup für jeden Core Server hinzuzufügen. Von einer Webkonsole können Sie diese Rollup-Skripts so planen, dass sie zum gewünschten Zeitpunkt und im gewünschten Intervall ausgeführt werden. Rollup-Skripts werden nur auf der Webkonsole angezeigt und sind auf dem Rollup-Core resident.

So starten Sie das Rollup-Tool

1. Führen Sie auf einem Rollup-Core das Rollup-Tool aus (\Programme\LANDesk\ManagementSuite\dbrollup.exe).
2. Wählen Sie einen vorhandenen Core Server, der verwaltet werden soll, aus der Liste aus, oder klicken Sie auf **Neu**, um den Namen eines neuen Rollup-Core einzugeben.
3. Sobald Sie einen Rollup-Core ausgewählt haben, werden in der Liste der Quell-Cores die Cores angezeigt, die Sie für den Rollup auf den ausgewählten Rollup-Core konfiguriert haben.

So konfigurieren Sie die Attribute, für die ein Rollup durchgeführt werden soll

1. Wählen Sie über das Rollup-Tool den Rollup-Core aus, den Sie konfigurieren möchten.
2. Klicken Sie auf **Attribute**.
3. Standardmäßig wird für alle Datenbankattribute ein Rollup durchgeführt. Verschieben Sie die Attribute, für die kein Rollup durchgeführt werden soll, von der Spalte **Ausgewählte Attribute** in die Spalte **Verfügbare Attribute**.
4. Klicken Sie auf **OK**, wenn Sie fertig sind. Wenn Attribute in die Spalte "Verfügbare Attribute" verschoben werden, werden verknüpfte Daten aus der Rollup-Datenbank gelöscht.

So konfigurieren Sie die Quell-Core Server für einen Rollup-Core

1. Wählen Sie über das Rollup-Tool den Rollup-Core aus, den Sie konfigurieren möchten.
2. Sobald Sie einen Rollup-Core ausgewählt haben, werden in der Liste der Quell-Cores die Cores angezeigt, die Sie für den Rollup auf den ausgewählten Rollup-Core konfiguriert haben. Klicken Sie auf **Hinzufügen**, um weitere Cores hinzuzufügen oder wählen Sie einen Core aus und klicken Sie auf **Löschen**, um einen Core zu löschen. Wenn Sie auf "Löschen" klicken, wird der ausgewählte Core sowie alle Core-Daten aus der Rollup-Datenbank entfernt.

So werden Datenbank-Rollup-Jobs auf der Webkonsole geplant

1. Wählen Sie über das Rollup-Tool den **Rollup-Core** aus, den Sie konfigurieren möchten.
2. Wählen Sie in der Liste **Quell-Cores** den Core aus, für den ein Rollup geplant werden soll und klicken Sie auf **Planen**. Wenn Sie keine Cores auswählen, wird die Planung für alle Cores in der Liste standardmäßig durchgeführt, wenn Sie auf **Planen** klicken. Wenn Sie auf **Planen** klicken, wird ein Rollup-Skript für den ausgewählten Core zum ausgewählten Rollup-Core hinzugefügt.
3. Stellen Sie von einer Webkonsole eine Verbindung zum Rollup-Core Server her.
4. Klicken Sie im linken Navigationsfenster auf **Planen von Rollup-Jobs**.
5. Klicken Sie auf das Rollup-Skript, für das Sie eine Planung durchführen möchten. Die Skriptnamen beginnen mit dem Quell-Core-Namen, gefolgt vom Namen des Ziel-Rollup-Core in Klammern. Klicken Sie auf **Rollup planen**.

6. Wählen Sie aus, wann der Rollup durchgeführt werden soll und ob er automatisch neu geplant werden soll oder nicht. Klicken Sie auf **Mit dem nächsten Schritt fortfahren**.
7. Prüfen Sie den Skriptplan und klicken Sie auf **Fertigstellen**.

Erhöhen des Rollup-Datenbank-Timeout

Bei großen Rollup-Datenbanken kann es zu einem Timeout des Webkonsolen-Abfrageeditors kommen, wenn eine lange Liste wie z.B. die Liste der Softwarepaketnamen angezeigt wird. Wenn dies der Fall ist, enthält die Liste, die Sie anzeigen möchten, keine Daten. Wenn es zu Timeouts kommt, müssen Sie den Datenbank-Timeout-Wert erhöhen. Der Wert muss überall geändert werden, wo der IIS-Dienst oder der Webkonsolenserver installiert wird. Unter dem folgenden Registrierungsschlüssel

```
HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core
```

muss ein neues DWORD, Timeout, mit einem Dezimalwert von 1800 hinzugefügt werden. Dieser Wert ist in Sekunden angegeben. Sie können diesen Wert basierend auf Ihren Abfragearten und der Datenbankleistung anpassen. Stoppen Sie IIS und starten Sie ihn neu, damit die Änderungen übernommen werden.

Informationen über das Rollup-Tool

Verwenden Sie das Datenbank-Rollup-Tool (auszuführen vom Rollup-Core), um Daten-Rollups von Core Servern zu verwalten.

- **Rollup-Core:** Sie können mehrere Rollup-Cores über das Rollup-Tool verwalten. Wählen Sie den Core aus, den Sie verwalten möchten. Zunächst müssen Sie ein Laufwerk für jeden Rollup-Core zuordnen.
- **Neu:** Klicken Sie auf "Neu", um einen neuen Rollup-Core hinzuzufügen, den Sie verwalten möchten. Zunächst müssen Sie ein Laufwerk für jeden hinzuzufügenden Rollup-Core zuordnen. Geben Sie den Computernamen des Rollup-Core ein und klicken Sie auf **OK**.
- **Attribute:** Klicken Sie auf "Attribute", um die Attribute auszuwählen, für die ein Rollup durchgeführt werden soll. Die Attributliste gilt global für alle Core Server, die der ausgewählte Rollup-Core verwendet. Verschieben Sie einzelne Attribute oder Attributstrukturen aus der Spalte "Ausgewählte Attribute" (für diese Attribute wird ein Rollup durchgeführt) in die Spalte "Verfügbare Attribute" (für diese Attribute wird kein Rollup durchgeführt).
- **Datenbank zurücksetzen:** Klicken Sie auf "Datenbank zurücksetzen", um die ausgewählte Rollup-Datenbank zurückzusetzen. Sämtliche Daten werden hierdurch gelöscht und alle Tabellen wieder aufgebaut.
- **Hinzufügen:** Klicken Sie auf "Hinzufügen", um einen Core hinzuzufügen, dessen Daten im ausgewählten Rollup-Core enthalten sein sollen.
- **Löschen:** Klicken Sie auf "Löschen", um den ausgewählten Core und dessen Daten aus der Datenbank des Rollup-Cores zu entfernen. **WARNUNG:** Durch diese Option werden die Daten des ausgewählten Core gelöscht, wenn Sie auf **OK** klicken. Daten von anderen Core Servern bleiben in der Rollup-Datenbank gespeichert.

- **Planen:** Klicken Sie auf "Planen", um ein Rollup-Skript für den ausgewählten Core hinzuzufügen. Wenn Sie im Feld "Quell-Cores" keinen Core ausgewählt haben, erstellt diese Option Rollup-Skripts für alle Cores im Feld "Quell-Cores".
- **Rollup:** Klicken Sie auf "Rollup", damit vom ausgewählten Core umgehend ein Rollup ausgeführt wird. Wenn Sie im Feld "Quell-Core" keinen Core ausgewählt haben, wird durch diese Schaltfläche umgehend ein Rollup aller Cores ausgeführt.
- **Schließen:** Klicken Sie auf "Schließen", um das Rollup-Tool" zu schließen.

Einrichten der Sicherheit auf Funktionsebene für Rollup-Datenbanken

Wenn Sie die Webkonsole mit einer Core-Datenbank verwenden, wird der Zugriff auf Funktionen und Clients anhand der rollenbasierten Verwaltungseinstellungen gesteuert, die Sie in der Management Suite-Konsole vorgenommen haben. Weitere Informationen finden Sie unter "Rollenbasierte Verwaltung" in Kapitel 1 des *Benutzerhandbuchs*. Wenn Sie die Webkonsole mit einer Rollup-Core-Datenbank verwenden und den Zugriff auf Funktionen für diese Rollup-Datenbank kontrollieren möchten, müssen Sie die Sicherheit auf Funktionsebene wie unten beschrieben einrichten.

Der Webkonsolenadministrator legt die Sicherheit auf Funktionsebene fest, indem er die Benutzer einer der während der Installation erstellten Gruppen zuweist. Standardmäßig haben alle Benutzer mit Administratorrechten auf dem Core Server automatisch Zugriff auf alle Webkonsolenfunktionen, die ihnen im Rahmen ihrer Webkonsolenlizenz zur Verfügung gestellt werden. Alle anderen Benutzer müssen den genannten Gruppen zugewiesen werden. Ansonsten wird ihnen der Zugriff auf die Funktionen verweigert. Die Gruppen sind folgende:

- **rc_user** für die Verwendung der Fernsteuerung. Ein Benutzer mit Administratorrechten muss zunächst den Remote Control Viewer auf den Computer herunterladen, bevor Benutzer in dieser Gruppe einen Client fernsteuern können.
- **sd_user** zum Anzeigen von Softwareverteilungsprotokollen, geplanten Aufträgen und Skripts. Zur weiteren Erhöhung der Sicherheit können diese Benutzer nur Einstellungen konfigurieren und Pakete verteilen, wenn sie Administratorrechte haben.
- **inv_user** zum Erstellen und Ausführen benutzerdefinierter Abfragen.
- **report_user** zum Anzeigen von Berichten und Konfigurieren der Berichtslayouts.

Diese Gruppen basieren auf Windows NT-Gruppen. Standardmäßig sind sie als lokale Gruppen auf dem Webserver eingerichtet. Sie können sie allerdings auch als globale Gruppen auf dem Domänencontroller einrichten.

Zuweisen von Benutzern

Sie können diesen Gruppen nur Domänenbenutzer zuweisen. Wenn Sie Benutzer zuweisen, die für den Webserver lokale Benutzer sind, werden sie nicht authentifiziert. Lokale Benutzer können sich als lokale Benutzer eines Webservers nicht bei einem Fernclient anmelden (in diesem Fall, um auf die Webkonsole zuzugreifen).

Standardmäßig hat jeder Benutzer in der Administratorgruppe automatisch Zugriff auf alle Webkonsolenfunktionen.

Einrichten der Authentifizierung

Um die Sicherheit auf Funktionsebene nutzen zu können, müssen Sie die Authentifizierung einrichten, indem Sie die anonyme Authentifizierung auf dem Webserver deaktivieren, die Aktivierung der Windows 2000 Sicherheit jedoch beibehalten (dies ist Integrierte Windows-Authentifizierung unter Windows 2000). Das Setup-Programm stellt diese Optionen in der Regel automatisch ein.

Arbeiten mit mehreren Cores

Nachdem Sie die Webkonsole auf einem Webserver installiert haben, können Sie die Konfigurationsdatei \Inetpub\wwwroot\remote\xml\core.asp bearbeiten, um eine Verbindung zu weiteren Datenbanken herzustellen. Standardmäßig verweist diese Datei nur auf den Core Server. Sobald Sie weitere Server hinzugefügt haben, können Sie anhand eines Dropdown-Listenfeldes in der Webkonsole eine Verbindung zu zusätzlichen Datenbanken herstellen. Wenn Sie die Informationen, auf die diese Datei verweist, ändern, müssen Sie die Datei core.asp aktualisieren.

Alle Einträge in der Datei core.asp müssen einzeilig sein. Mehrzeilige Einträge verursachen einen Fehler.

Es folgt eine Beispieldatei:

```
<?xml version="1.0" ?>

<core>

<cores>

<item name="CORE-TEST"  Server="CORE-TEST\LDMSData" Datenbank="lddb"
Benutzer="sa" Kennwort="" isoracle="0" Software="0" Rollup="0"/>

<Elementname="ROLLUP-TEST"  Server="ROLLUP-TEST" Datenbank="ldms"
Benutzer="sa" Kennwort="" isoracle="0" Software="0" Rollup="1"/>

</cores>

</core>
```

Eintrag	Beschreibung
Elementname=	Der Name des Servers, zu dem die Webkonsole eine Verbindung herstellen soll. Der hier angegebene Name wird auch in der Dropdown-Liste mit Datenbanken auf der Anmeldeseite der Webkonsole angezeigt.
Server=	Bei einem SQL-Server ist dies der Datenbankservername bzw. Datenbankinstanzname. Geben Sie keinen Datenbankinstanznamen an, wenn sich die entsprechende Datenbank in der Standard-SQL-Instanz befindet. Für Oracle ist dies die Oracle-Hostzeichenfolge (Dienst-/Instanzname).
Datenbank=	Der Name der SQL-Datenbank, den Sie auf dem Webserver erstellt haben. Für Oracle-Datenbanken ist diese Option leer.
Benutzer=	Die Standardbenutzerkennung für die Datenbank.
Kennwort=	Das mit der Standardbenutzerkennung verbundene Kennwort.
isoracle=	Gibt an, ob es sich bei der Datenbank um eine Oracle-Datenbank handelt (1) oder nicht (0).
Software=	Für eine zukünftige Verwendung. Lassen Sie das Feld leer.
Rollup=	Ob es sich bei der Datenbank um eine Core-Rollup-Datenbank handelt (1) oder nicht (0).

So fügen Sie Datenbanken zur Datei core.asp hinzu

1. Die Datei core.asp finden Sie auf dem Webserver in dem Verzeichnis, in dem die Webkonsole installiert ist (standardmäßig c:\\Inetpub\wwwroot\remote\xml).
2. Öffnen Sie die Datei core.asp in einem Texteditor, z. B. Notepad.
3. Kopieren Sie eine vorhandene Elementnamenzeile der Datei core.asp (ähnlich wie im Beispiel oben) und fügen Sie sie anschließend unterhalb des vorhandenen Textes ein. Ändern Sie die Zeilen den Daten der zusätzlichen Datenbank(en) entsprechend.
4. Speichern Sie die aktualisierte Datei core.asp als Textdatei.

Konfigurieren von Einstellungen

Bestimmen Sie durch das Konfigurieren von Einstellungen, wie die Webkonsole Informationen anzeigt. Klicken Sie auf **Konfigurieren > Einstellungen**, um die Seite "Einstellungen" zu öffnen.

Im Anfängermodus werden am oberen Rand der jeweiligen Seite Instruktionen eingeblendet, die Anweisungen zur Verwendung der Schaltflächen, Menüs und Dialogfelder enthalten. Zudem ist jede Schaltfläche in der Symbolleiste mit einem Namen versehen, aus dem hervorgeht, welche Aktion mit dieser Schaltfläche ausgeführt wird. Im Fortgeschrittenenmodus werden die auf den jeweiligen Seiten angezeigten Instruktionen ausgeblendet und nur Symbole - keine Namen - auf den Schaltflächen der Symbolleiste angezeigt.

Wenn Sie einen Bericht anzeigen, eine Abfrage ausführen oder mit der Funktion Computer suchen arbeiten, zeigt die Webkonsole eine Liste mit Rechnern und den von Ihnen angefordeten Inventarinformationen an. Je nach Monitorgröße und persönlichen Einstellungen und je nachdem, ob Sie Informationen drucken möchten, empfiehlt es sich möglicherweise für Sie, die Anzahl der Zeilen, die die Webkonsole auf der jeweiligen Seite anzeigt, zu ändern.

So konfigurieren Sie die Einstellungen

1. Klicken Sie in der Dropdown-Liste für den Anfängermodus auf **Lernen** und für den Fortgeschrittenenmodus auf **Expert**.
2. Geben Sie die Anzahl der Datenzeilen an, die pro Seite angezeigt werden sollen.
3. Klicken Sie in der Dropdown-Liste auf **3D-Tortendiagramm**, um Berichte als dreidimensionale Tortendiagramme aufzubereiten, auf **3D-Balkendiagramm**, um sie als dreidimensionale Balkendiagramme anzuzeigen, auf **2D-Tortendiagramm** für die Anzeige als zweidimensionale Tortendiagramme bzw. **2D-Balkendiagramm** für die Anzeige als zweidimensionale Balkendiagramme.
4. Klicken Sie auf **Aktualisieren**.

   Die neuen Einstellungen werden auf der Seite mit den aktualisierten Konsoleneinstellungen angezeigt.

Einstellungen werden als Cookies gespeichert.
Die Konsoleneinstellungen werden im Cookie-Verzeichnis des Webbrowsers gespeichert.

Tipps für die Fehlerkorrektur

Die folgenden Tipps für die Fehlerkorrektur beziehen sich auf Probleme, die am häufigsten im Zusammenhang mit der Webkonsole auftreten.

Nach der Anmeldung erscheint eine leere Seite und ich kann auf keinerlei Funktionen zugreifen.
Die Datei CORE.ASP enthält wahrscheinlich fehlerhafte Einträge. Bearbeiten Sie die Datei und stellen Sie sicher, dass die Daten zu der Datenbank, mit der Sie eine Verbindung herstellen möchten, korrekt sind.

Der Scanner kann keine Verbindung mit dem Server herstellen.
Wenn der Scanner keine Verbindung mit dem Server herstellen kann, überprüfen Sie, ob das Verzeichnis der Webanwendung korrekt konfiguriert ist. Wenn Sie https verwenden, benötigen Sie ein gültiges Zertifikat. Stellen Sie sicher, dass Sie ein gültiges Zertifikat besitzen.

Ich erhalte eine ungültige Sitzung beim Anzeigen der Webkonsole.
Es kann sein, dass die Browsersitzung abgelaufen ist. Klicken Sie auf **Anmelden** im linken Navigationsfenster, um eine neue Sitzung zu starten.

Das Sitzungstimeout für die Webkonsole läuft zu häufig ab.
Sie können das standardmäßige Sitzungstimeout für die Webseiten der Webkonsole ändern. Der IIS-Standard liegt bei 20 Minuten Inaktivität, bevor eine Anmeldung abläuft. So ändern Sie das IIS-Sitzungstimeout

1. Öffnen Sie auf dem Webserver den IIS Internetdienst-Manager.
2. Erweitern Sie die Standardwebsite.
3. Klicken Sie mit der rechten Maustaste auf den Ordner "Remote" und klicken Sie dann auf "Eigenschaften".
4. Klicken Sie in der Registerkarte "Verzeichnis" auf "Konfiguration".
5. Klicken Sie auf die Registerkarte "Anwendungsoptionen" und ändern Sie das Sitzungstimeout auf den gewünschten Wert.

Die Seite "Fernsteuerung" wird in der Webkonsole nicht angezeigt.
Um die Seite **"Fernsteuerung"** anzeigen zu können, müssen Sie ActiveX Controls aktivieren. Auf einigen Browsern sind ActiveX Controls standardmäßig deaktiviert. Wenn die Seite **"Fernsteuerung"** nicht ordnunsgemäß geladen wird, aktivieren Sie ActiveX Controls auf Ihrem Browser, indem Sie die Sicherheitseinstellungen ändern.

Ich habe die Schritte für die Softwareverteilung ausgeführt, aber die Webkonsole hat kein Paket erstellt.
Die Webkonsole verwendet die IUSR- und IWAM-Konten auf dem Webkonsolenserver. Diese Konten werden ursprünglich auf der Basis des Computernamens erstellt. Wenn Sie den Computernamen irgendwann einmal geändert haben, müssen Sie die unten genannten Schritte ausführen, um erfolgreich Softwareverteilungspakete zu erstellen.

1. Wenn auf Ihrem System .Net Framework installiert ist, deinstallieren Sie es.
2. Deinstallieren Sie IIS.
3. Installieren Sie IIS neu.
4. Installieren Sie .Net Framework neu, wenn Sie es deinstalliert haben.

Ein geplanter Softwareverteilungsauftrag wurde nicht ausgeführt.
Wenn Sie einen Softwareverteilungsauftrag planen und dieser nicht ausgeführt wird, stellen Sie sicher, dass der Intel Scheduler Service auf dem Server ausgeführt wird.

Die Inventardaten sind unvollständig.
Sie werden möglicherweise feststellen, dass bestimmte Inventardaten in Abfrageergebnissen oder Berichten nicht enthalten sind, wenn Sie zwischen Rollup-Datenbanken wechseln. Dieses Problem tritt auf , wenn mehrere Rollup-Datenbanken im Netzwerk vorhanden sind, die jeweils unterschiedlich strukturiert sind. Das Problem lässt sich verhindern, indem Sie benutzerdefinierte Daten nicht nur einer Rollup-Datenbank, sondern auch allen anderen hinzufügen.

Benutzerdefinierte Abfragen einer Oracle-Datenbank erzeugen eine Fehlermeldung, die besagt, dass die Seite nicht gefunden wurde.
Wenn Sie versuchen, benutzerdefinierte Abfragen zu verwenden, und diese Fehlermeldung erhalten, kann ein Oracle-Defekt die Fehlerursache sein. Führen Sie zur Fehlerkorrektur folgende Schritte aus:

1. Melden Sie sich bei Windows als ein Benutzer mit Administratorrechten an.
2. Starten Sie Windows-Explorer aus dem Menü "Start" und wählen Sie den Ordner ORACLE_HOME aus. In der Regel handelt es sich hierbei um den Ordner "Ora92", der dem Ordner "Oracle" untergeordnet ist (d. h. D:\Oracle\Ora92).
3. Klicken Sie im Kontextmenü des Ordners ORACLE_HOME auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Sicherheit**.
5. Klicken Sie in der Liste **Name** auf **Authentifizierte Benutzer**. Windows XP verwendet als Bezeichung für die Liste **Gruppen- oder Benutzernamen**.
6. Deaktivieren Sie in der Liste **Berechtigungen** unter **Zulassen** die Option **Lesen und Ausführen**. In Windows XP trägt die Liste **Berechtigungen** die Bezeichnung **Berechtigungen für authentifizierte Benutzer**.
7. Markieren Sie die Option **Lesen und Ausführen** erneut in der Spalte **Zulassen** (dieselbe Option, die Sie vorhin gerade deaktiviert haben).
8. Klicken Sie im Listenfeld **Berechtigungseinträge** auf **Erweitert** und überprüfen Sie, ob die hier aufgeführten **Authentifizierten Benutzer** über die Berechtigungen zum Lesen und Ausführen für diesen Ordner, Unterordner und Dateien verfügen. Sollte dies nicht der Fall sein, bearbeiten Sie die Zeile und stellen Sie sicher, dass das Feld **Übernehmen für** auf **Diesen Ordner, Unterordner und Dateien** gesetzt ist. Diese Einstellung sollte bereits korrekt vorgenommen worden sein, es ist aber wichtig, dass Sie dies überprüfen.
9. Klicken Sie so lange auf **OK**, bis Sie alle Sicherheitsdialogfelder geschlossen haben.
10. Starten Sie Ihren Server neu, um sicherzustellen, dass diese Änderungen wirksam werden.

Kapitel 8: Überwachen der Einhaltung von Softwarelizenzbestimmungen

Die Softwarelizenzüberwachung liefert Ihnen Tools zur Implementierung kompletter effektiver Softwarebestandsverwaltungs- und Lizenzbestimmungsrichtlinien.

Die Softwarelizenzüberwachung enthält folgende Funktionen:

- Funktion zum Scannen bekannter und unbekannter Anwendungen und ein Dispositionstool zur Definition und Verwaltung zuvor unbekannter Anwendungen.
- Anwendungsstartverweigerung, um die Ausführung nicht autorisierter Software zu verhindern - sogar auf Clients, die nicht mit dem Netzwerk verbunden sind.
- Vollständige Integration in LANDesk-Inventarverwaltung für aktuelle, komplette Informationen über installierte Anwendungen.
- Umfassende Berichte zur Anwendungsnutzung und zu Lizenzbestimmungen.
- Umfassende Funktionen zur Lizenzüberwachung und Berichtserstellung, einschließlich Informationen darüber, wie oft jede lizenzierte Anwendung aufgerufen wurde, Datum der letzten Verwendung und Gesamtdauer der Anwendungsnutzung.
- Einfache Konfiguration der Lizenzparameter, einschließlich gekaufter Anzahl, Lizenztyp, Menge und Seriennummer.
- Informationen zum Lizenzkauf, einschließlich Preis, Kaufdatum, Auftragsnummer und Wiederverkäuferdaten.
- Installationsverfolgung und -abstimmung, einschließlich Lizenzinhaber und physikalischer Standort des Clients, auf dem die Lizenz installiert ist, sowie weitere Informationen.
- Aliasnamen zur Verfolgung von Software, wenn sich Anbieterdaten oder Dateinamen ändern.

In diesem Kapitel erfahren Sie mehr über:

- Erstellen von Produkt- und Lieferantenaliasnamen
- Überwachung von Produkten hinsichtlich der Einhaltung von Lizenzbestimmungen
- Arbeitsweise der Erfüllungsüberwachung
- Informationen zur Strukturansicht "Erfüllung"
- Auswählen der zu überwachenden Produkte
- Downgroaden von Produktlizenzen
- Betrachten von Trends hinsichtlich der Einhaltung von Lizenzbestimmungen sowie der Verwendung und Verweigerung von Produkten
- Bearbeiten des Softwareinventars
- Informationen zu LDAPPL3
- Bearbeiten von LDAPPL3
- Hinzufügen von Dateien zu LDAPPL3
- Exportieren und Importieren von Daten aus dem Fenster "Softwarelizenzüberwachung"
- Verwenden der Softwarelizenzüberwachung mit Macintosh-Clients

Überwachen der Einhaltung von Softwarelizenzbestimmungen

Das Fenster "Softwarelizenzüberwachung" soll es Ihnen ermöglichen, die auf den Clients installierte Software zu überwachen und zu verwalten. Sie steuern das Fenster über den linken Fensterausschnitt, wo Sie in der Strukturansicht ""Softwarelizenzüberwachung" drei Haupt-Tasks bearbeiten können.

- **Aliase:** In dieser Ansicht können Sie Aliasnamen für Produkte oder Lieferanten definieren. Ein Alias gewährleistet, dass Sie auch dann über alle installierten ausführbaren Dateien eines bestimmten Lieferanten oder über ein Produkt genau Buch führen können, wenn sich der Lieferantenname ändert bzw. wenn sich der Lieferant oder der Name des Produkts ändert. Diese Funktion ist insbesondere dann hilfreich, wenn Sie in der Strukturansicht "Erfüllung" Produkte überwachen und genaue Daten zu den Lizenzen verwalten müssen.
- **Erfüllung:** In dieser Strukturansicht können Sie die Verwendung und Einhaltung der Lizenzbestimmungen von Produkten innerhalb Ihrer Organisation überwachen, des Downgroaden von Produktlizenzen konfigurieren, Clients die Verwendung von Anwendungen verweigern und Trends hinsichtlich der Erfüllung von Lizenzbestimmungen, der Verwendung und der Verweigerung von Anwendungen betrachten.
- **Inventar:** In dieser Baumansicht können Sie die Datei LDAPPL3, eine Softwarebeschreibungsdatei, die auf Ihrem Core Server gespeichert ist, bearbeiten. Der Inventarscanner identifiziert anhand der Datei LDAPPL3 das Softwareinventar Ihrer Clients.

Überdies können Sie Daten, die im Fenster "Softwarelizenzüberwachung" angezeigt werden, an andere Management Suite 7/8-Core Server in Ihrem Netzwerk exportieren und von dort importieren. Diese Funktion ist nützlich, wenn Sie sicherstellen müssen, dass die Core-Datenbanken auf allen Core Servern der Version 8 synchronisiert sind.

Erstellen von Produkt- und Lieferantenaliasnamen

Sie benutzen die Ansicht "Aliase" zum Erstellen von Produkt- oder Lieferantenaliasnamen. Ein Alias gewährleistet, dass Sie anhand folgender Daten über alle installierten Produkte korrekt Buch führen können:

- **Normalisierung der Daten zu ausführbaren Dateien:** Ein Alias trägt zur Konsistenz der Informationen bei, die zur korrekten Identifizierung eines Produkts von der Core-Datenbank benötigt werden. Beispielsweise sind die von einem Lieferanten bereitgestellten Dateiinformationen nicht immer konsistent. Wenn Dateien verschiedener Microsoft-Produkte in die Core-Datenbank eingelesen werden, kann der Lieferantenname möglicherweise Microsoft Corp, Microsoft (R) oder nur Microsoft lauten. Falls Sie dann eine Abfrage nach Produkten von "Microsoft (R)" ausführen, erhalten eine Liste, die lediglich einen Teil der in Ihrem Netzwerk installierten Microsoft-Produkte umfasst. Durch die Erstellung eines Lieferantenalias namens "Microsoft Corp" für alle in Ihrem Netzwerk installierten Microsoft-Produkte gewährleisten Sie, dass alle diese Produkte über denselben Lieferantennamen verfügen.
- **Aktualisierung der Daten zu ausführbaren Dateien:** Ein Alias ermöglicht es Ihnen, Dateiinformationen zu aktualisieren, falls sich der Produktname oder der Lieferant nach der Installation ändert. Beispielsweise ändern sich gelegentlich Lieferanten- oder Produktnamen, weil eine Firma übernommen oder veräußert wurde oder weil eine Firma ein Produkt nach einigen Versionen umbenannt hat. Wenn dieser Fall bei einer Ihrer Clientanwendungen eintritt, können Sie mithilfe von Aliasnamen die neuen Lieferanten- oder Produktnamen den ursprünglichen Namen zuordnen und damit sicherstellen, dass die Core-Datenbank die ausführbaren Dateien weiterhin korrekt identifizieren kann. Diese Funktion ist insbesondere dann hilfreich, wenn Sie in der Strukturansicht "Erfüllung" Produkte überwachen und genaue Daten zu den Lizenzen verwalten müssen.

Informationen zur Ansicht "Aliase"

Im rechten Fensterausschnitt der Ansicht "Aliase" werden der ursprüngliche Lieferanten- und Produktname sowie die von Ihnen hinzugefügten neuen Lieferanten- und/oder Produktnamen angezeigt. Es muss ein Softwarescan ausgeführt werden, bevor ein neuer Alias im Fenster "Softwarelizenzüberwachung" oder in Anlagenberichten erscheint, die Daten zu der auf den Clients installierten Software enthalten.

Sie können im Dialogfeld "Aliaseigenschaften" zwei Typen von Aliasnamen definieren:

- **Lieferant:** Ein Alias für alle installierten Produkte eines bestimmten Lieferanten (geben Sie den ursprünglichen Lieferantennamen und einen neuen Lieferantennamen ein).
- **Produkt:** Ein Alias für ein bestimmtes Produkt (geben Sie die ursprünglichen Lieferanten- und Produktnamen sowie neue Namen ein). Ein Produktalias, der einen neuen Lieferanten enthält, hat stets Vorrang vor einem Alias, der für sämtliche Produkte eines bestimmten Lieferanten definiert wurde.

Von Ihnen definierte Aliasnamen werden in den Strukturansichten "Aliase", "Erfüllung" und "Inventar" sowie in Anlagenberichten angezeigt, die Daten zur Clientsoftware enthalten.

So definieren Sie einen Alias

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie im linken Fensterausschnitt mit der rechten Maustaste auf **Aliase**, um das betreffende Kontextmenü zu öffnen, und klicken Sie in diesem Kontextmenü auf **Alias erstellen**.
3. Geben Sie im Dialogfeld **Aliaseigenschaften** den ursprünglichen Lieferantennamen und den ursprünglichen Produktnamen sowie den neuen Lieferanten- und/oder Produktnamen für die Anwendung ein. Klicken Sie auf **OK**.

So bearbeiten Sie einen Alias

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie im linken Fensterausschnitt auf **Aliase**.
3. Klicken Sie im rechten Fensterausschnitt im Kontextmenü für einen Alias auf **Eigenschaften**.
4. Bearbeiten Sie im Dialogfeld **Aliaseigenschaften** die Felder in der erforderlichen Weise. Klicken Sie auf **OK**.

So löschen Sie einen Alias

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie im linken Fensterausschnitt auf **Aliase**.
3. Klicken Sie im rechten Fensterausschnitt im Kontextmenü für einen Alias auf **Löschen**.

Nachdem Sie einen Alias gelöscht haben, werden nach dem nächsten Softwarescan wieder der ursprüngliche Lieferanten- und Produktname in der Core-Datenbank verwendet.

Informationen zum Dialogfeld "Aliaseigenschaften"

Sie verwenden das Dialogfeld "Aliaseigenschaften" (klicken Sie mit der rechten Maustaste auf einen Alias, und klicken Sie dann auf **Eigenschaften**), um einen Alias für die ausführbare Datei eines Produkts zu definieren. Durch die Verwendung von Aliasnamen wird sichergestellt, dass der Scanner Clientanwendungen richtig identifizieren kann, falls sich nach deren Installation Produkt- oder Lieferantennamen ändern.

Falls bei Ihrer Clientsoftware Namensänderungen auftreten, verknüpfen Sie die neuen Lieferanten- oder Produktnamen mithilfe von Aliasnamen mit den ursprünglichen Namen. Der Scanner ordnet die neuen Namen dann jeder ausführbaren Datei zu, die den ursprünglichen Daten in der Core-Datenbank des Core Servers entspricht, und stellt damit sicher, dass die Software korrekt identifiziert wird.

Diese Funktion ist besonders beim Überwachen von Produktlizenzen in der Ansicht "Erfüllung" hilfreich, da sie gewährleistet, dass der Scanner die betreffenden Produkte weiterhin erkennt.

- **Ursprünglicher Lieferant:** Geben Sie den Namen des ursprünglichen Lieferanten des Produkts ein.
- **Ursprünglicher Produktname:** Geben Sie den ursprünglichen Produktnamen ein.
- **Neuer Lieferant:** Geben Sie den neuen Lieferantennamen ein.
- **Neuer Produktname:** Geben Sie den neuen Namen des Produkts ein.

Überwachung von Produkten hinsichtlich der Einhaltung von Lizenzbestimmungen

Für IT-Administratoren ist es oft schwierig, den Einsatz von Produktlizenzen zu verfolgen, die auf vielen Clients innerhalb eines Netzwerks installiert sind. Sie laufen nicht nur Gefahr, Produktlizenzen zu häufig bereitzustellen, sondern auch, zu viele Lizenzen für Produkte zu kaufen, die sich als unnötig erweisen. Sie können diese Probleme vermeiden, indem Sie mithilfe der Strukturansicht "Erfüllung" den Einsatz von Produktlizenzen und die Verwendung von Produkten innerhalb Ihrer Organisation überwachen und die betreffenden Daten in Berichten zusammenstellen. Die Strukturansicht "Erfüllung" bietet folgende Funktionen:

- **Passive, minimale Bandbreite erfordernde Überwachung:** Der Softwarelizenzüberwachungsagent überwacht passiv die Produktverwendung auf Clients und belegt hierbei minimale Netzwerkbandbreite. Der Agent überwacht auch die Verwendung von Produkten auf mobilen Clients, die vom Netzwerk getrennt sind.
- **Berichte:** Die Leistungsfähigkeit dieser Überwachungsfunktion beruht auf ihren Datenerfassungsmöglichkeiten. Verwenden Sie die Daten, um die Erfüllung von Lizenzbestimmungen allgemein zu verfolgen und Trends hinsichtlich der Produktverwendung und -verweigerung zu beobachten.
- **Dwngroaden von Produktlizenzen:** Für bestimmte Produkte können Sie eines Lizenzdowngroaden einrichten, sodass eine Lizenz für neuere Versionen eines Produkts für ältere Versionen des Produkts verwendet werden kann und die Clientlizenzen somit jederzeit den Bestimmungen entsprechen.

Arbeitsweise der Erfüllungsüberwachung

Der Softwarelizenzüberwachungsagent wird im Rahmen des Standard-Client-Setup auf den Clients installiert. Der Agent zeichnet Daten über alle auf einem Client installierten Anwendungen auf und speichert diese Daten in der Systemregistrierung des Clients unter:

HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\Software Monitoring\MonitorLog

Im Fenster "Softwarelizenzüberwachung" können Sie die wichtigsten dieser installierten Anwendungen überwachen. Daten zur Verwendung von nicht überwachten Anwendungen werden ignoriert und in der Systemregistrierung des Clients schließlich durch neuere Daten überschrieben.

Nachdem Sie die zu überwachenden Anwendungen und Lizenzen angegeben haben, geschieht Folgendes:

- Management Suite sucht nach Clients, auf denen die zu überwachenden Anwendungen ausgeführt werden, und importiert diese Liste in das Fenster "Softwarelizenzüberwachung". Diese Clientliste bleibt unverändert, bis der nächste Softwarescan durchgeführt wird.

- Während der nächsten Überprüfung liest der Scanner die von den Softwarelizenzüberwachungsagenten erfassten Daten und sendet diese Daten an den Core Server. Management Suite aktualisiert dann das Fenster "Softwarelizenzüberwachung" mit den Daten zu den überwachten Lizenzen und Produkten.

Informationen zu mobilen Clients

Bei mobilen Clients, die vom Netzwerk getrennt sind, erfasst der Softwarelizenzüberwachungsagent weiterhin Daten und speichert diese in der Systemregistrierung des Clients. Sobald der Client wieder eine Netzwerkverbindung hergestellt hat, wird bei der nächsten Überprüfung erkannt, welche der zwischengespeicherten Daten überwacht werden, und diese Daten werden an den Core Server gesendet. Das Fenster "Softwarelizenzüberwachung" wird daraufhin mit den neuesten Daten zur Einhaltung von Lizenzbestimmungen, Verwendung und Verweigerung von Produkten für diese mobilen Clients aktualisiert.

Informationen zur Strukturansicht "Erfüllung"

In der Strukturansicht "Erfüllung" werden folgende Daten angezeigt:

- **Linker Fensterausschnitt:** Anzeige einer hierarchischen Strukturansicht von Produktgruppen, welche lizenzierte Produkte enthalten, die Sie überwachen möchten. Wenn Sie die Strukturansicht erweitern und unter einem bestimmten Produkt auf einen der folgenden Einträge klicken, werden im rechten Fensterausschnitt verschiedene Arten von Daten angezeigt:
    - **Dateien:** Dateien, die für ein bestimmtes Produkt überwacht werden. Dateien werden hier angezeigt, wenn Sie sie aus einer beliebige Kategorie unter **Inventar > Dateien** ziehen und hier ablegen. Sobald eine Datei hier angezeigt wird, wird sie auch in der Kategorie "In überwachtem Produkt" unter **Inventar > Ansichten** aufgeführt.
    - **Lizenzen:** Die Lizenzangaben für ein bestimmtes Produkt.
    - **Produkte Downgroaden:**Die Lizenzen, die für ein bestimmtes Produkt übernommen oder verliehen wurden. Wenn in Ihrem Netzwerk zwei Versionen desselben Produkts installiert sind, können Sie die ältere Version so konfigurieren, dass hierfür die Lizenz der neueren Version übernommen wird. Indem Sie die Möglichkeit zum Downgroaden wahrnehmen, können Sie verhindern, dass bei der alten Version die Höchstzahl lizenzierter Benutzer überschritten wird.
    - **Verwendungsbericht:**Clientdaten zur Verwendung eines bestimmten Produkts.
    - **Verweigerungsbericht:**Daten zur verweigerten Verwendung eines bestimmten Produkts.
- **Rechter Fensterausschnitt:** Abhängig von Ihrer Auswahl im linken Fensterausschnitt, werden in diesem Fensterausschnitt ausführbare Dateien von überwachten Produkten, Informationen zur Erfüllung von Lizenzbestimmungen, zu Lizenzen downgroaden oder zur Produktverwendung bzw. der verweigerten Verwendung von Produkten angezeigt.

Auswählen der zu überwachenden Produkte

Damit Produkte hinsichtlich der Einhaltung von Lizenzbestimmungen und Verwendungs-/Verweigerungstrends überwacht werden können, müssen Sie im Fenster "Softwarelizenzüberwachung" drei verschiedene Arbeitsgänge abschließen:

1. Einrichten einer Strukturansicht für Produktgruppen und einzelne Produkte
2. Auswählen der zu überwachenden Produktdateien
3. Hinzufügen der Produktlizenzdaten

Einrichten der Strukturansicht

Sie richten im linken Fensterausschnitt unter "Erfüllung" eine hierarchische Strukturansicht der Produktgruppen und einzelnen Produkte ein. Sie können Produkte beliebig gruppieren, zum Beispiel:

- Nach Firmennamen, wie z. B. Adobe oder Microsoft
- Nach bestimmten Kategorien, wie z. B. "Nicht autorisierte Dateien" oder "Buchhaltungsabteilung"
- Nach Produktsuite, wie z. B. Microsoft Office

In diese Gruppen fügen Sie die Produkte ein, deren Verwendung oder verweigerte Verwendung überwacht werden soll. Sie können beispielsweise der Gruppe "Adobe" Produkte wie Photoshop* und Illustrator* hinzufügen.

Während der Installation werden standardmäßig diese Produktgruppen erstellt, um Ihnen den Einstieg zu erleichtern:

- **LANDesk Management Suite 7.0:** Diese Gruppe enthält Produkt- und Dateicontainer für Management Suite 7.0. Sie müssen lediglich Ihre Lizenzinformationen eingeben, damit die Erfüllung der Lizenzbestimmungen von Management Suite 7.0 auf den Clients überwacht wird.
- **LANDesk Management Suite 8:** Diese Gruppe enthält Produkt- und Dateicontainer für Management Suite 8. Sie müssen lediglich Ihre Lizenzinformationen eingeben, damit die Einhaltung der Lizenzbestimmungen von Management Suite 8 auf Ihren Clients überwacht wird.
- **Microsoft Office:** Diese Gruppe enthält Produkt- und Dateicontainer für Office* 2000 Premium und Office XP Professional. Sie müssen lediglich Ihre Lizenzinformationen eingeben, damit die Einhaltung der Lizenzbestimmungen von Microsoft Office auf Ihren Clients überwacht wird.

So stellen Sie die Standardeinstellungen der Strukturansicht wieder her
Falls Sie diese vorgegebenen Gruppen einmal löschen sollten und sie später wieder verwenden möchten, importieren Sie einfach die Datei DEFAULTS.XML aus dem Ordner C:\Programme\LANDesk\ManagementSuite\ldlogon Ihres Core Servers. Durch den Import dieser XML-Datei in das Fenster "Softwarelizenzüberwachung" werden die Produktgruppen sowie die ursprünglichen Daten der Datei LDAPPL3, die zum Lieferumfang von Management Suite 7 gehört, wiederhergestellt. Ein XML-Import bewirkt, dass diese Daten mit den in den Strukturansichten "Erfüllung" und "Inventar" des Fensters bereits vorhandenen Daten zusammengeführt werden.

So richten Sie eine Strukturansicht ein

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie im Kontextmenü für **Erfüllung** auf **Neue Gruppe**.
3. Geben Sie den Namen der neuen Produktgruppe ein.
4. Um Produkte in diese Gruppe einzufügen, klicken Sie mit der rechten Maustaste auf den Gruppennamen und wählen eine der folgenden Optionen:

    - **Neues Produkt:**Wenn Sie ein Produkt hinzufügen möchten, bei dem Sie Trends hinsichtlich seiner Verwendung überwachen möchten.
    - **Neues verweigertes Produkt:**Wenn Sie ein Produkt hinzufügen möchten, bei dem Sie Trends hinsichtlich seiner Verweigerung überwachen möchten.

5. Geben Sie den Produktnamen ein. Nach dieser Eingabe werden Ihnen folgende Änderungen auffallen:

    - Unter einem neuen Produkt werden die Container "Dateien", "Lizenzen", "Produkte downgroaden", "Verwendungsbericht" und "Verweigerungsbericht" angezeigt. Sie können dem Container "Dateien" ausführbare Dateien und dem Container "Lizenzen" Lizenzinformationen hinzufügen. Falls dieses Produkt die Möglichkeit zum Downgroaden der Lizenz bietet, können Sie diese konfigurieren, indem Sie auf den Container "Produkte downgroaden" klicken.
    - Unter einem gerade verweigerten Produkt werden die Container "Dateien", "Lizenzen", "Produkte downgroaden", "Verwendungsbericht" und "Verweigerungsbericht" angezeigt. Sie können die ausführbaren Dateien zuerst zum Container "Dateien" und anschließend zur Kategorie **Inventar > Dateien > Zu verweigern** hinzufügen. Beachten Sie, dass Sie ausführbare Dateien in einem verweigerten Produkt nicht zur Kategorie **Zu verweigern** hinzufügen müssen. Sie werden verweigert, wenn das Produkt mit **Verwendung dieses Produkts verweigern** markiert ist.

So bearbeiten Sie die Strukturansicht

- So bearbeiten Sie die Eigenschaften eines Produkts: Klicken Sie im linken Fensterausschnitt mit der rechten Maustaste auf den Produktnamen, und klicken Sie dann im Kontextmenü auf **Eigenschaften**. Geben Sie den Produktnamen, die Version und den Herstellernamen ein; geben Sie an, ob Clients die Verwendung dieses Produkts verweigert werden soll und ob alle zu diesem Produkt gehörigen Dateien auf dem Client installiert sein müssen, bevor eine Lizenz als genutzt bewertet wird. Klicken Sie auf **OK**.
- So löschen Sie eine Produktgruppe oder ein Produkt oder benennen diese um: Klicken Sie im linken Fensterausschnitt mit der rechten Maustaste auf den Namen der Produktgruppe oder des Produkts, und klicken Sie dann im Kontextmenü auf **Löschen** oder **Umbenennen**.

Informationen zum Dialogfeld "Produkteigenschaften"

Im Dialogfeld "Produkteigenschaften" (klicken Sie mit der rechten Maustaste auf ein Produkt, und klicken Sie dann auf **Eigenschaften**) können Sie die Eigenschaften des gewählten Produkts betrachten und ändern.

- **Produktname:** Name des Produkts, dessen Eigenschaften angezeigt werden.
- **Version:** Zeigt die Versionsnummer des Produkts.
- **Verleger:** Lieferant, der das Produkt hergestellt hat.
- **Verwendung dieses Produkts verweigern:** Angabe, ob die Softwarelizenzüberwachung Clients die Ausführung dieses Produkts verweigern soll.
- **Alle Dateien abgleichen:** Angabe, ob mehrere Dateien auf dem Client vorhanden sein müssen, bevor eine Lizenz als verwendet gilt.

Auswählen der zu überwachenden Produktdateien

Sie wählen aus den Kategorien der Strukturansicht "Inventar" die zu überwachenden Produktdateien aus. Sobald Sie eine Datei in der Strukturansicht "Erfüllung" überwachen, wird diese Datei auch in der Kategorie **Inventar > Ansichten > In überwachtem Produkt** angezeigt.

So wählen Sie die zu überwachenden Produktdateien aus

1. Klicken Sie auf **Erfüllung > Produktgruppe > Produkt**.
2. Klicken Sie im Kontextmenü für **Dateien** auf **Dateien hinzufügen**.
3. Geben Sie in das Feld **Suchen** ein Wort ein, und legen Sie dann mithilfe des Dropdown-Menüs **In Spalte** fest, ob das angegebene Wort Bestandteil des Lieferanten-, Produkt- oder Dateinamens der Datei ist. Sie können auch mithilfe des Dropdown-Menüs **Dateiliste** die Kategorie der Strukturansicht "Inventar" angeben, die Sie durchsuchen möchten.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Suche**.
5. Wählen Sie die Datei in der Ergebnisliste aus, und klicken Sie dann auf **Hinzufügen**, um die Datei der Dateiliste dieses Produkts hinzuzufügen.

Nachdem Sie die Dateien hinzugefügt haben, ermittelt Management Suite sofort die Clients, auf denen die betreffenden ausführbaren Dateien ausgeführt werden (nach Maßgabe des letzten Softwarescans), und überträgt diese Daten in das Fenster "Softwarelizenzüberwachung". Nach dem nächsten Softwarescan können Sie dem Verwendungsbericht entnehmen, welche Clients die Datei(en) ausgeführt haben, bzw. im Verweigerungsbericht sehen, welche Clients versucht haben, die Datei(en) auszuführen. Um diese Clients anzuzeigen, klicken Sie auf **Erfüllung > Produktgruppe > Produkt > Verwendungsbericht** oder **Verweigerungsbericht**.

Über die Option "In Produkt suchen" können Sie außerdem herausfinden, welche Produkte dieselbe Version einer Datei verwenden.

So finden Sie heraus, welche Produkte eine Datei verwenden

1. Klicken Sie auf **Erfüllung > Produktgruppe > Produkt > Dateien**.
2. Wählen Sie die Datei, nach der Sie suchen möchten, und klicken Sie im Kontextmenü auf **In Produkt suchen**. Im Menü wird Ihnen nun angezeigt, welche Produkte dieselbe Datei und Dateiversion enthalten. Wenn Sie auf ein Produkt klicken, gelangen Sie zu der Datei in diesem Produkt.

So finden Sie heraus, wo Dateien auf den Clients installiert sind

1. Klicken Sie auf **Erfüllung > Produktgruppe > Produkt > Dateien**.
2. Wählen Sie die Datei, nach der Sie suchen möchten, und klicken Sie im Kontextmenü auf **Wo installiert**.

Informationen zum Fenster "Dateien zum Produkt hinzufügen"

Im Fenster "Dateien zum Produkt hinzufügen" (klicken Sie mit der rechten Maustaste auf ein Produkt, und klicken Sie dann auf **Dateien hinzufügen**) geben Sie an, welche Dateien überwacht werden sollen, um festzustellen, ob ein Produkt ausgeführt wird.

- **Suchen:** Geben Sie den Dateinamen oder den Suchbegriff ein, nach dem gesucht werden soll.
- **In Spalte:** Wählen Sie die Inventarspalte aus, die Sie durchsuchen möchten; Lieferant, Produktname, Dateiname, Version und Größe stehen zur Auswahl.
- **Ermittelt, aber nicht in Produkt:** Zeigt Dateien an, die auch in der Liste "Zur Disposition" aufgeführt, aber gegenwärtig in der Strukturansicht "Erfüllung" nicht überwacht werden. Dieser Liste können Sie Dateien entnehmen, die möglicherweise hinsichtlich der Einhaltung von Lizenzbestimmungen und Trends zur Verwendung/Verweigerung überwacht werden sollten.
- **Zu prüfen:** Zeigt Dateien an, die in der Datei LDAPPL3 des Core Servers enthalten sind und die vom Scanner auf den Clients identifiziert werden können.
- **Zur Disposition:** Zeigt Dateien an, die auf den Clients erkannt wurden, aber in der Datei LDAPPL3 nicht enthalten sind. Sie müssen diese Dateien in andere Kategorien verschieben, damit der Scanner sie identifizieren kann.
- **Auf Computern ermittelt:** Zeigt sämtliche Dateien an, die auf den Clients erkannt wurden, auch wenn sie zu Produkten gehören, die in der Datei LDAPPL3 nicht definiert sind.
- **In überwachtem Produkt:** Zeigt Dateien an, die bereits zur Überwachung von Produkten verwendet werden.
- **Fensterbereich "Dateiinformationen":** Zeigt Dateien an, die dem Suchbegriff und der gewählten Dateiliste entsprechen.

Hinzufügen der Produktlizenzdaten

Sie müssen Lizenzinformationen hinzufügen, damit die Einhaltung der Lizenzbestimmungen für ein Produkt überwacht werden kann. Falls Sie lediglich die Produktverwendung nachverfolgen möchten, können Sie diesen Schritt übergehen.

Nachdem Sie die Lizenzinformationen für ein Produkt angegeben haben, wird durch ein rotes Symbol mit einem Ausrufezeichen neben einer Produktgruppe angezeigt, dass ein Produkt dieser Gruppe nicht den Lizenzbedingungen entsprechend verwendet wird. Erweitern Sie die Produktgruppe, um das betreffende Produkt ausfindig zu machen, und betrachten Sie die zugehörigen Informationen im rechten Fensterausschnitt.

So fügen Sie Produktlizenzdaten hinzu

1. Klicken Sie auf **Erfüllung > Produktgruppe > Produkt**.
2. Klicken Sie im Kontextmenü für **Lizenzen** auf **Neue Lizenz**.
3. Geben Sie auf den Registerkarten des Dialogfelds "Lizenzeigenschaften" die Informationen zu Lizenz, Kauf und Verfolgung ein, die für Ihre Organisation relevant sind.
4. Nach der Eingabe aller erforderlichen Daten klicken Sie auf **OK**.
5. Wenn Sie sicherstellen möchten, dass alle zu einem Produkt gehörigen ausführbaren Dateien auf einem Client installiert sind, bevor die Einhaltung der Lizenzbestimmungen für das betreffende Produkt überwacht wird, können Sie im linken Fensterausschnitt mit der rechten Maustaste auf den Produktnamen klicken und die Option **Alle Dateien abgleichen** wählen. Weitere Informationen zur Option "Alle Dateien abgleichen" finden Sie im nächsten Abschnitt.

Informationen zum Dialogfeld "Lizenzeigenschaften"

Das Dialogfeld "Lizenzeigenschaften" besitzt drei Registerkarten:

- Lizenz
- Kaufdaten
- Verfolgen

Auf der Registerkarte "Lizenz" konfigurieren Sie die Lizenzeigenschaften des Produkts.

- **Lizenznummer:** Geben Sie hier eine gültige Lizenznummer für das Produkt ein.
- **Lizenztyp:** Geben Sie den Typ der Lizenz an, die Sie für das Produkt besitzen, z. B.: Kostengünstiges Upgrade, Freeware, Neuerwerb, OEM, Produktupgrade, Public Domain, Shareware, unbekannt.
- **Menge:** Geben Sie die Anzahl der von Ihnen erworbenen Produktlizenzen ein.
- **Seriennummer:** Geben Sie hier eine zusätzliche Nummer ein, die zur Produktlizenz gehört.

Auf der Registerkarte "Kaufdaten" konfigurieren Sie die Kaufmerkmale der Produktlizenz.

- **Kaufdatum:** Geben Sie das Datum ein, an dem das Produkt von Ihrem Unternehmen gekauft wurde.
- **Stückpreis:** Geben Sie den Preis jeder für dieses Produkt erworbenen Lizenz ein.
- **Bestellnummer:** Geben Sie die für den Kauf verwendete Bestellnummer ein.

- **Wiederverkäufer:** Geben Sie den Namen des Händlers ein.

Auf der Registerkarte "Verfolgen" konfigurieren Sie die Eigenschaften des Produkts, die zur Nachverfolgung dienen.

- **Besitzer:** Geben Sie die Person oder Abteilung Ihrer Firma ein, die für die Aufbewahrung des verpackten Produkts verantwortlich ist.
- **Ort:** Geben Sie den Ablageort an, an dem das verpackte Produkt aufbewahrt wird.
- **Hinweis:** Geben Sie zusätzliche Informationen zur Produktlizenz ein, z. B. Möglichkeiten der Lizenzdowngroaden.

Überwachen von Lizenzen mithilfe der Option "Alle Dateien abgleichen"

Gelegentlich kann es vorkommen, dass Sie Lizenzen von zwei oder mehr Produkten überwachen müssen, deren ausführbare Dateien denselben Namen und dieselbe Größe haben. In einem solchen Fall müssen Sie zusätzlich eine Datei überwachen, die in den einzelnen Produkten eindeutig ist. Durch die Auswahl der Option "Alle Dateien abgleichen" und den Einsatz der ausführbaren Datei sowie einer einzigartigen Datei zum Erkennen einer Lizenznutzung legen Sie fest, dass alle zu dem Produkt gehörigen Dateien (die sich in dessen Container "Dateien" befinden) auf einem Client installiert sein müssen, bevor die Produktlizenz als genutzt gilt. Damit wird sichergestellt, dass der Scanner die Produktlizenzen korrekt nachverfolgen kann.

Anhand der folgenden beiden Beispiele wird erläutert, wann Sie die Option "Alle Dateien abgleichen" verwenden:

- Wenn Sie die Lizenzverwendung für MSDE und SQL 2000 überwachen und beide Produkte eine Datei SQLSERVR.EXE derselben Größe verwenden, sollten Sie auch eine .DLL oder eine andere Anwendungsdatei überwachen, die jedem dieser Produkte eigen ist. Diese anderen Dateien werden von Management Suite nicht hinsichtlich der Einhaltung der Lizenzbestimmungen überwacht (dies geschieht nur bei ausführbaren Dateien); sie erleichtern es dem Scanner lediglich, die MSDE-Lizenz von der SQL 2000-Lizenz zu unterscheiden.

  Hinweis: Wenn Sie Dateien, die keine .EXE-Dateien sind, einem Produkt hinzufügen (um die Option "Alle Dateien abgleichen" verwenden zu können), müssen Sie zuerst die Datei LDAPPL3.TEMPLATE bearbeiten, damit diese bei Softwarescans berücksichtigt werden. Per Voreinstellung berücksichtigt LDAPPL3 nur ausführbare Dateien. Weitere Informationen hierzu finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE" in Anhang A.

- Wenn Sie 10 Lizenzen für Office XP Standard (enthält Word, Excel, Outlook und PowerPoint) sowie 10 Lizenzen für Office XP Pro (enthält dieselben Anwendungen plus Access) überwachen, stellt sich Ihnen das Problem, dass Sie zwei verschiedene Produktlizenzen überwachen möchten, die gleichnamige und gleich große ausführbare Dateien umfassen. Der Scanner kann Lizenztypen weder anhand einzelner Dateien noch durch den Einsatz der Option "Alle Dateien abgleichen" bei beiden Produkten unterscheiden.

  Sie müssen in diesem Fall einen Schritt weiter gehen und eine ausführbare Datei von Office XP Pro dem Container "Dateien" von XP Standard hinzufügen und diese ausführbare Datei durch Auswahl von **Nicht in Produkt**. **als nicht zum Produkt gehörig markieren.** Damitwird sichergestellt, dass der Softwarelizenzüberwachungsagent keine Office XP Pro-Lizenz als XP Standard-Lizenz verzeichnet, was der Fall wäre, wenn lediglich die Option "Alle Dateien abgleichen" ausgewählt würde.

So markieren Sie eine ausführbare Datei als nicht zum Produkt gehörig:

1. Markieren Sie die Datei im rechten Fensterausschnitt.
2. Drücken Sie die rechte Maustaste, und wählen Sie **Nicht in Produkt**.

Downgroaden von Produktlizenzen

Im Fenster "Softwarelizenzüberwachung" können Sie die Lizenzen für bestimmte Produkte "downgroaden". Wenn in Ihrem Netzwerk zwei Versionen desselben Produkts installiert sind, können Sie die ältere Version so konfigurieren, dass hierfür die Lizenz der neueren Version ausgeliehen wird.

Indem Sie die Möglichkeit zum Downgroaden wahrnehmen, können Sie verhindern, dass bei der alten Version die Höchstzahl lizenzierter Benutzer überschritten wird. Beispielsweise könnten Sie Office XP so konfigurieren, dass Lizenzen für Office 97 bereitgestellt werden, falls die Office 97-Lizenzen erschöpft sind, und damit sicherstellen, dass Clients Office 97-Anwendungen weiterhin unter Einhaltung der Lizenzbestimmungen ausführen können. Ein Nachteil ist, dass Lizenzen nicht in der umgekehrten Richtung ausgeliehen werden können, sodass die neuere Version eine Lizenz von einer älteren Version übernimmt.

Diese Funktion ist nur bei Produkten einsetzbar, bei denen der Hersteller des Downgroaden von Lizenzen erlaubt. Die Firma Microsoft lässt dies beispielsweise bei vielen ihrer Produkte zu. Wenn Sie sich vergewissern möchten, ob eines Lizenzdowngroaden bei einem Produkt zulässig ist, schlagen Sie in der Lizenzvereinbarung des Produkts nach.

Die folgenden Szenarien beschreiben (neben dem oben genannten), wann Sie Lizenzen downgroaden können:

- Produkt #1 und #2 übernehmen die Lizenz von Produkt #3: Beispielsweise können Sie Office 97 und Office 2000 so konfigurieren, dass für diese Produkte Office XP-Lizenzen benutzt werden.
- Produkt #1 übernimmt Lizenzen von Produkt #2 und Produkt #3: Beispielsweise können Sie Office 97 so konfigurieren, dass für dieses Produkt Office 2000- und Office XP-Lizenzen benutzt werden.

- Produkt #1 übernimmt Lizenzen von Produkt #2, und Produkt #2 übernimmt Lizenzen von Produkt #3. Beispielsweise können Sie Office 97 so konfigurieren, dass für dieses Produkt Office 2000-Lizenzen verwendet werden, und dann Office 2000 so konfigurieren, dass hierfür Office XP-Lizenzen benutzt werden.

Zu eine Produktlizenz downgroaden

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Erfüllung > Produktgruppe > Produkt > Produkte downgroaden**.
3. Klicken Sie auf **Hinzufügen**. Wählen Sie ein Produkt aus, dem Sie Lizenzen verleihen können, und klicken Sie dann auf **Hinzufügen**.
4. Wiederholen Sie Schritt 3, um ein zweites oder drittes Produkt für die Lizenzübernahme zu konfigurieren. Die Reihenfolge, in der die downgroaden Produkte in der Liste angegeben sind, ist wichtig. Weiter unten in der Liste aufgeführte Produkte erhalten nur dann Lizenzen, wenn die Produkte über ihnen noch nicht alle verfügbaren Lizenzen verwendet haben. Um ein Produkt in der Liste nach oben oder unten zu verschieben, markieren Sie es und klicken dann auf **Nach oben** bzw. **Nach unten**.

Das Downgroaden von Lizenzen beginnt nach dem nächsten Softwarescan; Sie können dies in dieser Ansicht verfolgen. Informationen über das Produkt werden in den Listen unter "Downgroadete lizenzierte Produkte" und "Hochgestufte lizenzierte Produkte" angezeigt.

Informationen zum Fenster "Produkte downgroaden"

Im Fenster "Produkte downgroaden" (klicken Sie in der Strukturansicht auf ein Produkt und dann auf **Produkte downgroaden**) konfigurieren Sie die für die Nachverfolgung relevanten Eigenschaften einer Produktlizenz.

- **Lizenzen:** Zeigt die Gesamtanzahl der Lizenzen an, die von Produkten verfügbar sind, von denen Lizenzen übernommen werden.
- **Installationen:** Zeigt an, wie viele Lizenzen für das Produkt, das gerade konfiguriert wird, verwendet werden.
- **Schaltfläche "Hinzufügen":** Klicken Sie auf diese Schaltfläche, um anzugeben, welche Produkte von dem Produkt, das Sie gerade konfigurieren, Lizenzen übernehmen können.
- **Schaltfläche "Entfernen":** Klicken Sie auf diese Schaltfläche, um ein Produkt aus der Liste zu entfernen.
- **Schaltflächen "Nach oben" und "Nach unten":** Markieren Sie ein Produkt in der Liste "Downgroadete lizenzierte Produkte", und klicken Sie auf **Nach oben** oder **Nach unten**, um die Rangfolge des Produkts bei der Vergabe geliehener Lizenzen festzulegen.

Betrachten von Trends hinsichtlich der Einhaltung von Lizenzbestimmungen sowie der Verwendung und Verweigerung von Produkten

Eine der mächtigsten Funktionen des Fensters "Softwarelizenzüberwachung" besteht in der Fähigkeit, die Erfüllung der Lizenzbestimmungen im Allgemeinen sowie Trends hinsichtlich der Verwendung und der Verweigerung von Produkten zu verfolgen. Die folgenden Arten von Daten werden im rechten Fensterausschnitt der Strukturansicht "Erfüllung" angezeigt:

- **Erfüllung von Lizenzbestimmungen allgemein** Anzeige von allgemeinen Daten zur Einhaltung der Lizenzbestimmungen aller definierten Produktgruppen
- **Erfüllung der Lizenzbestimmungen von Produktgruppen:** Anzeige von auf einzelne Gruppen bezogenen Daten zur Einhaltung der Lizenzbestimmungen von Produktgruppen
- **Produktverwendungsbericht:** Anzeige von auf einzelne Clients bezogenen Daten zur Produktverwendung
- **Produktverweigerungsbericht:** Anzeige von auf einzelne Clients bezogenen Daten zu ausführbaren Dateien, deren Verwendung verweigert wurde

So betrachten Sie allgemeine Daten zur Erfüllung der Lizenzbestimmungen

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Erfüllung**. Daraufhin werden im rechten Fensterausschnitt für alle definierten Gruppen allgemeine Daten zur Erfüllung der Lizenzbestimmungen angezeigt, wie z. B.:

   - **Produktgruppe:** Namen der definierten Produktgruppen
   - **Erfüllt:** Angabe, ob die Lizenzbestimmungen einer Produktgruppe erfüllt werden
   - **Keine Erfüllung:** Anzahl der Lizenzen innerhalb einer Produktgruppe, die nicht den Bestimmungen entsprechend verwendet werden
   - **Nicht bereitgestellte Lizenzen:** Anzahl der Lizenzen für eine Produktgruppe, die nicht verwendet werden

So zeigen Sie die Erfüllung der Lizenzbestimmungen innerhalb einzelner Produktgruppen an

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Erfüllung > Produktgruppe**. Daraufhin werden im rechten Fensterausschnitt für die gewählte Gruppe allgemeine Daten zur Erfüllung der Lizenzbestimmungen angezeigt, wie z. B.:

   - **Lizenziertes Produkt:** Namen der Produkte innerhalb dieser Gruppe
   - **Lizenzen:** Anzahl von Lizenzen, die in Ihrer Organisation für Produkte dieser Gruppe zur Verfügung stehen
   - **Installationen:** Anzahl der Installationen, die gegenwärtig auf Clients für Produkte dieser Gruppe eingerichtet sind
   - **Keine Erfüllung:** Anzahl der Lizenzen, die gegenwärtig auf Clients verwendet werden und nicht den Lizenzbestimmungen entsprechen

- **Nicht bereitgestellte Lizenzen:** Anzahl der Lizenzen, die nicht für Produkte dieser Gruppe verwendet werden
- **Verliehen:** Anzahl der Lizenzen, die von diesem Produkt an eine ältere Version desselben Produkts verliehen wurden
- **Geliehen:** Anzahl der Lizenzen, die von diesem Produkt von einer neueren Version desselben Produkts ausgeliehen wurden
- **Ungenutzt:** Anzahl der Clients, die das installierte Produkt bislang nicht ausgeführt haben

So betrachten Sie einen Bericht über die Produktverwendung

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Erfüllung > Produktgruppe > Produkt > Verwendungsbericht**. Daraufhin werden im rechten Fensterausschnitt allgemeine Daten zur Verwendung des betreffenden Produkts angezeigt, wie z. B.:

   - **Rechner:** Name des Clients
   - **Zuletzt verwendet:** Zeitpunkt, zu dem diese .EXE-Datei zuletzt auf dem Client ausgeführt wurde
   - **Letzter Benutzer:** Benutzername des Benutzers, der sich zuletzt bei diesem Client angemeldet hat
   - **Anzahl Ausführungen:** Anzeige, wie oft die .EXE-Datei auf dem Client ausgeführt wurde
   - **Dauer (Minuten):** Anzeige, wie viele Minuten lang die .EXE-Datei auf dem Client ausgeführt wurde
   - **Letztes Rücksetzdatum:** Zeitpunkt, zu dem diese Daten zuletzt aus der Core-Datenbank und der Registrierungsdatenbank des Clients gelöscht wurden (indem mit der rechten Maustaste auf **Erfüllung** geklickt und **Verwendungsdaten zurücksetzen** gewählt wurde). Dieses Datum wird vom Core Server bereitgestellt.

Sie können diese Spalten sortieren, indem Sie auf die Spaltenüberschrift klicken. Wenn Sie mit der rechten auf einen Clientnamen klicken, wird ein Fenster geöffnet, in dem das Inventar des betreffenden Clients angezeigt wird.

So zeigen Sie einen Bericht über die Produktverweigerung an

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Erfüllung > Produktgruppe > Produkt > Verweigerungsbericht**. Daraufhin werden im rechten Fensterausschnitt Daten zur verweigerten Ausführung der betreffenden .EXE-Datei angezeigt, wie z. B.:

   - **Rechner:** Name des Clients
   - **Letzter Benutzer:** Benutzername des Benutzers, der sich zuletzt bei diesem Client angemeldet hat
   - **Anzahl Verweigerungen:** Angabe, wie oft versucht wurde, die .EXE-Datei auf dem Client auszuführen

- **Letztes Rücksetzdatum:** Zeitpunkt, zu dem diese Daten zuletzt aus der Core-Datenbank und der Registrierungsdatenbank des Clients gelöscht wurden (indem mit der rechten Maustaste auf **Erfüllung** geklickt und **Verwendungsdaten zurücksetzen** gewählt wurde). Dieses Datum wird vom Core Server bereitgestellt.

Sie können diese Spalten sortieren, indem Sie auf die Spaltenüberschrift klicken. Wenn Sie mit der rechten auf einen Clientnamen klicken, wird ein Fenster geöffnet, in dem das Inventar des betreffenden Clients angezeigt wird.

Drucken oder Exportieren von Daten im Form von Berichten

Sie können sämtliche Daten der Strukturansicht "Erfüllung" in Form eines Berichts ausdrucken und in verschiedene Dateitypen (z. B. Crystal Reports*, Adobe Acrobat*, Microsoft Excel* etc.) exportieren.

So drucken oder exportieren Sie Daten

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Erfüllung**, und erweitern Sie die Strukturansicht, sodass die Produktdaten angezeigt werden, die Sie drucken oder exportieren möchten. (Diese Daten werden im rechten Fensterausschnitt angezeigt.)
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Drucken**, um die Daten im Berichtsformat zu öffnen.
4. Um den Bericht zu drucken, klicken Sie in der Symbolleiste auf die Schaltfläche **Drucken**.

Berichtsdaten zur Verwendung und Verweigerung von Produkten zurücksetzen

Sie können die Daten löschen, die in den Verwendungs- und Verweigerungsberichten überwachter Produkte enthalten sind. Durch die Löschung der Daten wird der Zähler zurückgesetzt, sodass Sie mit der Überwachung von Anwendungen neu beginnen können. Die Zurücksetzung betrifft alle Clients und bewirkt, dass sämtliche vorhandene Daten zu Verwendungs- und Verweigerungsberichten aus den Registrierungsdatenbanken der Clients und der Core-Datenbank entfernt werden. Aus diesem Grund sollten Sie alle Berichte, die Sie aufbewahren möchten, vor dem Zurücksetzen ausdrucken oder speichern. Wenn Sie die Verwendungs- und Verweigerungsberichtsdaten zurücksetzen, sind davon sämtliche überwachten Produkte in der Strukturansicht "Erfüllung" betroffen.

So setzen Sie Berichtsdaten zur Verwendung und Verweigerung von Produkten zurück

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie mit der rechten Maustaste auf **Erfüllung**, und wählen Sie **Verwendungsdaten zurücksetzen**.
3. Beantworten Sie die Eingabeaufforderung mit **Ja**, um die Zurücksetzung abzuschließen.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen**, damit den Clients die letzten Änderungen zur Verfügung stehen, wenn sie das nächste Mal einen Inventarscan durchführen.

Nach der Zurücksetzung müssen Sie einen Scan erzwingen, damit die Berichtsdaten aus den Registrierungsdatenbanken der Clients entfernt werden; anschließend müssen Sie einen zweiten Scan erzwingen, damit die neuen Daten im Fenster "Softwarelizenzüberwachung" angezeigt werden.

Bei großen Datenbanken kann die Zurücksetzung länger dauern. Wenn das Zeitlimit für die Zurücksetzung überschritten wird, kann Ihr Datenbankadministrator durch die Eingabe der folgenden SQL-Befehle die Verwendung manuell zurücksetzen:

```
UPDATE FileInfoInstance
SET SCM_TotalSessionTime = NULL,
SCM_SessionCount = NULL,
SCM_SessionsDenied = NULL,
SCM_LastUser = NULL,
SCM_LastSessionTime = NULL
```

Informationen zum Dialogfeld "Dateieigenschaften verweigern"

Im Dialogfeld "Dateieigenschaften verweigern" können Sie der Kategorie "Zu verweigern" der Strukturansicht "Inventar" Dateien hinzufügen. Wenn die Verwendung einer Datei verweigern, werden alle Dateien dieses Namens, ungeachtet unterschiedlicher Größe und Version, in diese Kategorie verschoben. Der Inventarscanner verhindert dann, dass irgendeine Datei dieses Namens ausgeführt wird.

Geben Sie den Dateinamen mit der Dateierweiterung ein.

Informationen zum Dialogfeld "Datei ausschließen"

In diesem Dialogfeld können Sie der Kategorie "Auszuschließen" der Strukturansicht "Inventar" Dateien hinzufügen. Wenn Sie eine Datei ausschließen, werden alle Dateien dieses Namens, ungeachtet unterschiedlicher Größe und Version, in diese Kategorie verschoben. Der Inventarscanner ignoriert dann alle Vorkommen dieses Dateinamens.

Geben Sie den Dateinamen mit der Dateierweiterung ein.

Bearbeiten des Softwareinventars

Mithilfe der Strukturansicht "Inventar" im Fenster "Softwarelizenzüberwachung" können Sie die Datei LDAPPL3 bearbeiten, eine Softwarebeschreibungsdatei, die auf Ihrem Core Server gespeichert wird. Der Inventarscanner identifiziert anhand der in LDAPPL3 enthaltenen Daten das Softwareinventar Ihrer Clients. Der Scanner erkennt Softwareanwendungen an drei Dingen:

- Dateiname
- Dateiname und Größe
- Informationen, die in der ausführbaren Datei der Anwendung enthalten sind

Informationen zur Strukturansicht "Inventar"

Die Strukturansicht "Inventar" enthält zwei Fensterausschnitte, in denen folgende Detaildaten angezeigt werden:

- **Linker Fensterausschnitt:** Dieser Fensterausschnitt enthält eine Strukturansicht für "Dateien" und "Ansichten".
    - **Dateien:** Anzeige der Kategorien, die Sie zur Strukturierung der Dateien, die in der Datei LDAPPL3 des Core Servers verzeichnet sind, verwenden können.
        - **Zu prüfen:** Dateien, die in der Datei LDAPPL3 des Core Servers enthalten sind und vom Scanner auf den Clients identifiziert werden können.
        - **Zur Disposition:** Dateien, die auf den Clients ermittelt wurden, aber in der Datei LDAPPL3 nicht enthalten sind. Sie müssen diese Dateien in andere Kategorien verschieben, damit der Scanner sie identifizieren kann.
        - **Auszuschließen:** Der Scanner ignoriert alle Vorkommen einer Datei, die Sie hierhin verschieben. Wenn Sie eine Datei aus der Liste "Auszuschließen" löschen, wird sie in der Kategorie "Zur Disposition" angezeigt.
        - **Zu verweigern:** Die Ausführung wird bei allen Vorkommen einer Datei, die Sie hierhin verschieben, verweigert. Benutzer, die versuchen, eine verweigerte ausführbare Datei auszuführen, sehen, dass das Programm einige Sekunden lang ausgeführt und dann beendet wird. Wenn Sie eine Datei aus der Liste "Zu verweigern" löschen, wird sie in der Kategorie "Zur Disposition" angezeigt.
    - **Ansichten:** Zeigt die folgenden Dateilisten im rechten Fensterausschnitt an:
        - **Ermittelt, aber nicht in Produkt:** Dateien, die auch in der Liste "Auf Computern ermittelt" aufgeführt, aber gegenwärtig in der Strukturansicht "Erfüllung" nicht überwacht werden. Dieser Liste können Sie Dateien entnehmen, die möglicherweise hinsichtlich der Einhaltung von Lizenzbestimmungen und Trends zur Verwendung/Verweigerung überwacht werden sollten.

   - **Auf Computern ermittelt:** Alle ausführbaren Dateien, die auf Clients ermittelt wurden, unabhängig davon, ob sie in der Datei LDAPPL3 enthalten sind. Sie können die Spalten im rechten Fensterausschnitt sortieren, um den Status der einzelnen Dateien klarer überblicken zu können, z. B. ob es sich um ein überwachtes Produkt handelt oder ob die Datei in einer LDAPPL3-Kategorie enthalten ist. Wenn erkannte Dateien den Status "Zur Disposition" besitzen, bedeutet dies, dass Sie in einem Softwarescan ermittelt wurden, aber nicht in LDAPPL3 enthalten sind. Dateien müssen in LDAPPL3 enthalten sein, bevor sie auf Clients regelmäßig gescannt, ausgeschlossen oder verweigert werden können.
   - **In überwachtem Produkt:** Dateien, die in der Strukturansicht "Erfüllung" auf die Erfüllung der Lizenzbestimmungen und Trends hinsichtlich der Verwendung oder Verweigerung hin überwacht werden. Sie können diese Dateien nicht aus der Strukturansicht "Inventar" heraus verschieben; sie werden lediglich zur Referenz angezeigt.
- **Rechter Fensterausschnitt:** Der Inhalt dieses Fensterausschnitt ändert sich, abhängig von Ihrer Auswahl im linken Fensterausschnitt.

Informationen zu LDAPPL3

Bei der Datei LDAPPL3 handelt es sich um die Nachfolgeversion der Datei LDAPPL.INI, die mit älteren Versionen von Management Suite ausgeliefert wurde. Anders als in der Vergangenheit sollten Sie diese Datei nicht mit einem Texteditor direkt bearbeiten, weil die Daten jetzt in Form einer komprimierten Datei in der Core-Datenbank des Core Servers gespeichert werden. Wenn der Server eine neue Version dieser Datei schreibt, gehen Änderungen, die Sie direkt mit einem Editor vorgenommen haben, verloren. Alle Änderungen an Softwarebeschreibungen, die in LDAPPL3 enthalten sind, müssen im Fenster "Softwarelizenzüberwachung" vorgenommen werden.

Die zum Lieferumfang von Management Suite gehörende Datei LDAPPL3 umfasst mehrere Tausend Anwendungen und stellt somit eine Grundmenge an ausführbaren Dateien bereit, die auf Ihren Clients installiert sein können. In diesem Fenster wählen Sie die ausführbaren Dateien aus, die in LDAPPL3 aufgeführt sind und die der Scanner auf Clients erkennen oder ausschließen oder deren Ausführung Clients verweigert werden soll. Falls eine ausführbare Datei nicht in LDAPPL3 enthalten ist, können Sie sie hinzufügen.

Standardmäßig enthält LDAPPL3 nur Beschreibungen ausführbarer Dateien. Falls der Scanner auch andere Typen von Anwendungsdateien (.DLL-, .COM-, .SYS-Dateien usw.) erkennen soll, können Sie diese Dateien manuell zu einer der Kategorien unter der Strukturansicht "Inventar > Dateien" hinzufügen, *nachdem* Sie die Datei DAPPL3.TEMPLATE so bearbeitet haben, dass alle Dateien dieses Typs bei einer Überprüfung berücksichtigt werden. Weitere Informationen hierzu finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE" in Anhang A.

Ab Management Suite 8 kann der Inventarscanner HTTP für LDAPPL3-Dateitransfers verwenden. Dadurch unterstützt der Scanner Targeted Multicast-Funktionen wie Polite-Bandbreite und Peer Download. Ein Peer Download ermöglicht Clients, die LDAPPL3-Updates benötigen, auf dem Core Server nach dem Datum der neuesten Version zu suchen. Anschließend stellen die Clients eine Verbindung zu Peers im Subnetz her, um zu ermitteln, ob ein Peer das Update in seinem Multicast-Cache hat. Verfügt ein Peer über das Update, erfolgt der Dateitransfer im lokalen Subnetz ohne Erzeugung von Netzwerkverkehr über Router oder WAN-Verbindungen. Weitere Informationen zu Targeted Multicast und Peer Downloads finden Sie unter "Verwenden von Targeted Multicasting mit Enhanced Software Distribution" in Kapitel 6.

Herunterladen aktualisierter LDAPPL3-Dateien
Sie können aktualisierte LDAPPL3-Dateien im XML-Format von der Website des LANDesk-Supports herunterladen. Besuchen Sie http://support.landesk.com/support, und wählen Sie dann die Verknüpfung zur Download-Seite für Management Suite 8.

Bearbeiten von LDAPPL3

Per Voreinstellung werden während der Installation von Management Suite anhand von LDAPPL3 Dateien in die Kategorien "Zu prüfen" und "Auszuschließen" unter **Inventar > Dateien** aufgenommen. Aus diesen Kategorien können Sie LDAPPL3 bearbeiten, indem Sie über das Kontextmenü einer ausführbaren Datei eine neue Kategorie auswählen.

Nachdem Sie die Datei LDAPPL3 des Core Servers bearbeitet haben, müssen Sie die letzten Änderungen den Clients für den nächsten Inventarscan zur Verfügung stellen. Sie tun dies, indem Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen** klicken. Daraufhin wird die Datei LDAPPL3 des Core Servers um 70 Prozent komprimiert, wodurch der Scanner die entsprechende LDAPPL3-Datei der Clients aktualisieren kann, ohne nennenswerte Bandbreite zu benötigen. (Die Datei LDAPPL3 der Clients wird im Rahmen des Standard-Client-Konfigurationssetup installiert.) Die Clientversionen und Core Server-Versionen dieser Datei müssen synchronisiert werden, damit der Scanner weiß, welche der zu überprüfenden Dateien auf den Clients zu ermitteln, auszuschließen oder zu verweigern sind.

Wenn Sie nicht abwarten möchten, bis die Datei LDAPPL3 durch den nächsten Inventarscan auf den Clients aktualisiert wird, können Sie Clients auf folgende Weise diese Änderungen zur Verfügung stellen:

- **Mithilfe der Anmeldeskripts der Clients:** Sie können im Clientsetup-Assistenten angeben, dass bei jedem Neustart des Clients automatisch Aktualisierungen der .INI-Datei des Core Servers in die lokale LDAPPL3-Datei des Clients übernommen werden.
- **Durch Planen einer Aufgabe, mit der LDAPPL3 mittels Push an Clients übertragen wird:** Sie verwenden das Fenster "Geplante Aufgaben", um einen Zeitpunkt festzulegen, zu dem die LDAPPL3-Datei des Core Servers an jeden Client übermittelt werden soll. Standardmäßig befindet sich die Datei LDAPPL3 im Ordner C:\Programme\LANDesk\ManagementSuite\LDLogon auf Ihrem Core Server.

- **Durch automatische Aktualisierung von LDAPPL3 während eines Inventarscans:** Um die LDAPPL3-Datei von Clients automatisch während eines Inventarscans zu aktualisieren, fügen Sie einen /i-Schalter zu der Verknüpfung hinzu, die den Inventarscanner auf den Clients startet.

So bearbeiten Sie die Datei LDAPPL3 des Core Servers

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Inventar > Dateien** und dann auf **Zu prüfen**, um die Liste der ausführbaren Dateien anzuzeigen, die der Scanner aktuell auf Clients ermittelt, oder klicken Sie dann auf **Auszuschließen**, um die Liste der ausführbaren Dateien anzuzeigen, die der Scanner gegenwärtig auf Clients ignoriert. Während der Einrichtung von Management Suite werden zwei LDAPPL.INI-Kategorien per Vorgabe mit Einträgen gefüllt.
3. Blättern Sie im rechten Fensterausschnitt nach unten, um die Dateien zu orten, die Sie in eine andere Kategorie unter "Inventar > Dateien" verschieben möchten. Oder suchen Sie nach Dateien, indem Sie einen vollständigen Dateinamen oder mithilfe des Platzhalterzeichens (*) ein Dateinamensmuster in das Feld **Suchen** eingeben und in der Symbolleiste auf die Schaltfläche **Suche** klicken. Die gesuchte ausführbare Datei sollte am Anfang der Liste angezeigt werden. Sie können LDAPPL3 bearbeiten, indem Sie über das Kontextmenü einer ausführbaren Datei eine neue Kategorie auswählen.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen**, damit den Clients die letzten Änderungen zur Verfügung stehen, wenn sie das nächste Mal einen Inventarscan durchführen, falls der Scannerbefehlszeilenparameter /i auf Clients verwendet wird.

Hinzufügen von Dateien zu LDAPPL3

Wenn Sie einer LDAPPL3-Kategorie neue Dateien hinzufügen müssen, können Sie dies auf zweierlei Weise tun.

Hinzufügen einzelner Dateien

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie auf **Inventar > Dateien** und anschließend auf die LDAPPL3-Kategorie, der die Datei hinzugefügt werden soll. Eine Beschreibung dieser Kategorien finden Sie weiter oben in diesem Kapitel unter "Informationen zur Strukturansicht "Inventar"".
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Datei**.
4. Geben Sie im Dialogfeld "Dateieigenschaften" den Dateinamen und die Eigenschaften ein, oder suchen Sie nach der Datei. Wenn Sie die Datei per Durchsuchen auswählen, werden Dateiname und Größe automatisch in die betreffenden Felder eingetragen. Wenn Sie Dateien zu den Listen "Ausgeschlossen" oder "Verweigert" hinzufügen, geben Sie den Dateinamen ein.
5. Klicken Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen**, damit den Clients die letzten Änderungen zur Verfügung stehen, wenn sie das nächste Mal einen Inventarscan durchführen.

Hinzufügen mehrerer Dateien

Durch die Ausführung eines Softwarescans mit der Option Mode=ALL können Sie nicht nur alle Clientanwendungsdateien ermitteln, die gegenwärtig in LDAPPL3 enthalten sind, sondern auch alle anderen, nicht in LDAPPL3 verzeichneten ausführbaren Dateien. Die unbekannten Dateien werden in die Kategorie "Zur Disposition" eingetragen, von wo Sie sie in andere LDAPPL3-Kategorien verschieben können.

Zur Ausführung eines Softwarescans mit der Option Mode=ALL müssen Sie die Datei LDAPPL3.TEMPLATE bearbeiten, die sich im Ordner C:\Programme\LANDesk\ManagementSuite\LDLogon des Core Servers befindet. Weitere Informationen hierzu finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE" in Anhang A.

Informationen zum Dialogfeld "Dateieigenschaften"

Im Dialogfeld "Dateieigenschaften" (klicken Sie auf **Inventar > Dateien >**, anschließend auf die Kategorie "Zu prüfen" oder "Zur Disposition" und dann in der Symbolleiste auf die Schaltfläche **Neue Datei**) können Sie einer LDAPPL3-Kategorie Dateien hinzufügen.

- **Schaltfläche "Durchsuchen":** Sie verwenden diese Schaltfläche, um eine Datei direkt auszuwählen. Wenn eine Datei auf diese Weise ausgewählt wird, werden die Felder "Dateiname" und "Größe" automatisch ausgefüllt.
- **Dateiname:** Geben Sie einen Dateinamen ein.
- **Größe (in Byte):** Geben Sie die Dateigröße in Byte an. Trennen Sie die Ziffern nicht durch Punkte oder andere Trennzeichen.
- **Produktname:** Geben Sie den Namen des Produkts ein, zu dem diese Datei gehört.
- **Lieferant:** Geben Sie den Namen des Lieferanten des Produkts ein, zu dem diese Datei gehört.
- **Version:** Geben Sie eine Versionsbezeichnung für die Datei ein.
- **Aktion oder Status:** Wählen Sie aus, was mit dieser Datei geschehen soll:
    - **Zu prüfen:** Fügen Sie die Datei dieser Kategorie hinzu, wenn der Inventarscanner auf Clients nach dieser Datei suchen soll.
    - **Zur Disposition:** Fügen Sie die Datei zu dieser Kategorie hinzu, wenn Sie später entscheiden möchten, was Sie mit dieser Datei tun möchten.
- **Prüfmethode:** Da Sie die Dateieigenschaften von LDAPPL3 bearbeiten, können Sie die Prüfmethode nicht ändern.

Exportieren und Importieren von Daten aus dem Fenster "Softwarelizenzüberwachung"

Sie können Daten, die im Fenster "Softwarelizenzüberwachung" angezeigt werden, an andere Management Suite 7 und 8-Core Server in Ihrem Netzwerk exportieren und von dort importieren. Diese Funktion ist nützlich, wenn Sie sicherstellen müssen, dass die Core-Datenbanken auf allen Core Servern der Management Suite 8 synchronisiert sind.

Sie können die Daten, die im Fenster unter "Alias", "Erfüllung" und "Inventar" angezeigt werden, in eine .XML-Datei *exportieren*, um sie in die Core-Datenbank eines anderen Core Servers importieren zu können.

Sie können eine .XML-Datei von einer anderen im Netzwerk vorhandenen Konsole *importieren*. Wenn importierte .XML-Dateien Aktualisierungen zu in der Core-Datenbank vorhandenen Daten enthalten, werden die vorhandenen Daten überschrieben. Neue Daten werden an die vorhandenen angehängt.

So exportieren Sie Daten aus LDAPPL3 in eine .XML-Datei

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Exportieren**, und speichern Sie die .XML-Datei an einem Ort, von dem Sie sie einfach in die Core Datenbank eines anderen Core Servers importieren können.

So importieren Sie eine .XML-Datei mit LDAPPL3-Daten

1. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Importieren**, und wählen Sie eine LDAPPL3-Datei oder eine .XML-Datei aus, die die Daten enthält, die Sie in die Core-Datenbank dieses Core Servers importieren möchten.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen**, damit den Clients die letzten Änderungen zur Verfügung stehen, wenn sie das nächste Mal einen Inventarscan durchführen, falls der Scannerbefehlszeilenparameter /i auf Clients verwendet wird.

Importieren einer alten LDAPPL.INI-Datei in das Fenster "Softwarelizenzüberwachung"

In Management Suite 6.62 und älteren Versionen hieß die Softwarebeschreibungsdatei LDAPPL.INI. Falls Sie eine alte LDAPPL.INI-Datei besitzen, die in den Abschnitten [Applications] und [Ignore] Softwarebeschreibungen enthält, die Sie in das Fenster "Softwarelizenzüberwachung" importieren möchten, dann können Sie dies tun, jedoch ist das entsprechende Verfahren etwas zeitaufwändig.

Sie müssen zuerst die Softwarebeschreibungen im Abschnitt [Applications] bearbeiten, die Sie in die neuere LDAPPL3-Datei importieren möchten. Sie können auch Softwarebeschreibungen aus dem Abschnitt [Ignore] importieren, die Sie vor dem Import nicht bearbeiten müssen. Obwohl die alte Datei LDAPPL.INI neben anderen Daten sowohl Software- als auch Hardwarebeschreibungen enthielt, werden lediglich die Softwarebeschreibungen aus diesen beiden Abschnitten in das Fenster "Softwarelizenzüberwachung" importiert.

Importieren benutzerdefinierter Hardwareinformationen
Falls die alte LDAPPL.INI-Datei, die Sie importieren möchten, auch benutzerdefinierte Hardwareinformationen (z. B. BIOS-Informationen) enthält, dann müssen Sie diese Daten der Datei LDAPPL3.TEMPLATE direkt hinzufügen. Weitere Informationen hierzu finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE" in Anhang A.

In der alten LDAPPL.INI-Datei müssen zwei Dinge bearbeitet werden, damit die Daten das für den Import in die neuere LDAPPL3-Datei erforderliche Format haben.

- Im Abschnitt [LANDesk Inventory] — Aktualisieren Sie die Zeilen für Version und Revision
- Im Abschnitt [Applications] —Teilen Sie bei jeder Anwendung den Eintrag für Lieferant/Produkt durch ein Komma in zwei Einträge auf, einen Eintrag für den Lieferanten und einen für das Produkt. Beispiel:

  In der alten LDAPPL.INI-Datei hat eine Zeile folgenden Inhalt:

```
<I>, EXCEL.EXE, 9165128, Microsoft Excel, 3.0a
```

  Sie müssen die Zeile wie folgt abändern (indem Sie Microsoft (Lieferant) und Excel (Produkt) durch ein Komma voneinander trennen):

```
<I>, EXCEL.EXE, 9165128, Microsoft, Excel, 3.0a
```

WICHTIG!
Wenn Sie Softwarebeschreibungen aus einer alten LDAPPL.INI-Datei in das Fenster "Softwarelizenzüberwachung" importieren, dann müssen Sie die Daten *genau* wie oben beschrieben abändern. **Erstellen Sie unbedingt eine Sicherungskopie von Ihrer Datenbank, bevor Sie die nachfolgenden Schritte ausführen**. Ein besseres Verfahren für den Import von Softwarebeschreibungen besteht darin, die Dateien einzeln den Kategorien in der Strukturansicht "Inventar > Dateien" hinzuzufügen. Weitere Informationen zu diesem Verfahren finden Sie unter "Hinzufügen von Dateien zu LDAPPL3" weiter oben in diesem Kapitel.

So importieren Sie eine alte LDAPPL.INI-Datei in das Fenster "Softwarelizenzüberwachung"

Erstellen Sie eine Sicherungskopie der ursprünglichen LDAPPL.INI-Datei, bevor Sie nachfolgende Schritte ausführen.

1. Öffnen Sie LDAPPL.INI im Editor oder in einem anderen Texteditor.
2. Suchen Sie im Abschnitt [LANDesk Inventory] nach den Zeilen für Version und Revision.
3. Ändern Sie den Eintrag in der Zeile **Version** in **3.0** und den Eintrag in der Zeile **Revision** in **1.00**.

4. Bearbeiten Sie im Abschnitt [Applications] der Datei die Softwarebeschreibungen, die Sie importieren möchten. Vergewissern Sie sich anhand des oben dargestellten Beispiels davon, dass Sie die Softwarebeschreibungseinträge korrekt bearbeiten.
5. Löschen Sie alle Softwarebeschreibungen aus den Abschnitten [Applications] und [Ignore], die nicht importiert werden sollen.
6. Speichern Sie die Datei, und beenden Sie den Editor.
7. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
8. Klicken Sie im Fenster "Softwarelizenzüberwachung" in der Symbolleiste auf die Schaltfläche **Importieren**.
9. Klicken Sie im Feld **Dateien vom Typ** auf **LDAPPL3-Dateien**, und wählen Sie dann das Verzeichnis der von Ihnen gespeicherten .INI-Datei aus.
10. Markieren Sie die Datei, und klicken Sie dann auf **Öffnen**, um die bearbeiteten Softwarebeschreibungen in das Fenster "Softwarelizenzüberwachung" zu importieren. Überprüfen Sie, ob die importierten Softwarebeschreibungen in die betreffenden Kategorien der Strukturansicht "Inventar > Dateien" importiert worden sind.

    - Aus dem Abschnitt [Applications] in die Kategorie "Zu prüfen"
    - Aus dem Abschnitt [Ignore] in die Kategorie "Auszuschließen"
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen**, damit den Clients die letzten Änderungen zur Verfügung stehen, wenn sie das nächste Mal einen Inventarscan durchführen.

Verwenden der Softwarelizenzüberwachung mit Macintosh-Clients

Macintosh-Clients (nur Mac OS 10.2+) unterstützen ebenfalls die Softwarelizenzüberwachung. Der Macintosh-Softwarelizenzüberwachungsagent sendet bei jedem Inventarscan Informationen über auf Clients ausgeführten Anwendungen an den Core Server. Das Softwarelizenzüberwachungsfenster zeigt Macintosh-Anwendungen und Windows-Anwendungen. Sie können die Ausführung von Macintosh-Anwendungen verweigern, indem Sie die Macintosh-Anwendungen in die Liste "Zu verweigern" aufnehmen.

Macintosh-Anwendungen sind in der LDAPPLl3.INI-Datei noch nicht enthalten. Sie müssen den Modus der LDAPPL3-Datei auf "Alle" oder "Nicht aufgeführt" setzen, damit Macintosh-Anwendungen in der Datenbank enthalten und verfügbar sind. Wenn Sie der Meinung sind, dass alle Macintosh-Anwendungen vorhanden sind, können Sie den Modus wieder auf "Aufgeführt" zurücksetzen.

Macintosh-Clients zeigen auf der Registerkarte "Softwarelizenzüberwachung" des Fensterbereichs für die Management Suite-Einstellungen an, welche Anwendungen installiert sind und wie oft sie verwendet wurden. Diese Registerkarte zeigt auch gesperrte Anwendungen an, die auf dem Client nicht gestartet werden.

Informationen zum Dialogfeld "Dateieigenschaften"

Im Dialogfeld "Dateieigenschaften" (klicken Sie in der Strukturansicht "Inventar" mit der rechten Maustaste auf eine Datei, und klicken Sie dann auf **Eigenschaften**) können Sie die Eigenschaften einer in der LDAPPL3-Datei des Core Servers verzeichneten Datei betrachten und ändern. Sie können nach Dateien suchen, die Sie LDAPPL3 hinzufügen möchten, und vorhandene Dateiinformationen bearbeiten.

- **Dateiname:** Name der Datei.
- **Größe (in Byte):** Größe der Datei.
- **Produktname:** Name der Anwendung, die von dieser Datei ausgeführt wird.
- **Lieferant:** Hersteller oder Lieferanten der Anwendung.
- **Version:** Versionsnummer der Datei.
- **Aktion oder Status:** Inventarkategorie, der diese Datei hinzugefügt werden soll.
- **Prüfmethode:** Methode, die vom Scanner zur Ermittlung dieser Datei eingesetzt wird.
    - **LdAppl3.ini verwenden:** Die Daten zu Dateiname, Größe, Anwendung und Version werden aus der Softwarebeschreibungsdatei LDAPPL3 übernommen. Dies ist die Standardprüfmethode.
    - **Daten aus Dateikopf verwenden:** Dateibeschreibung und -version werden aus dem Dateikopf der ausführbaren Datei übernommen.
    - **Produktname aus Dateikopf verwenden:** Produktname und -version werden aus dem Dateikopf der ausführbaren Datei übernommen.

Kapitel 9: Verteilen von Betriebssystemabbildern und Migrieren von Profilen

Mit den LANDesk Management Suite-Modulen für die Betriebssystem-Verteilung und Profilmigration können Sie Ihrem Netzwerk automatisierte Fernfunktionen für die Abbildbereitstellung und die Client-Profilmigration hinzufügen. Mit der Betriebssystem-Verteilung und der Profilmigration wird die Bereitstellung neuer Clients und die Migration vorhandener Clients optimiert. Sobald der Prozess gestartet wurde, sind keine weiteren Aktionen des Endbenutzers oder der IT-Abteilung erforderlich.

Sie können festlegen, dass Bereitstellungen und Migrationen erst nach Ablauf einiger Stunden erfolgen. Wenn Sie Abbilder mit Hilfe der Targeted Multicasting-Technologie von LANDesk verteilen, benötigen Sie nur ein Minimum an Netzwerkbandbreite, weil ein Abbild mehreren Clients bereitgestellt wird.

Hinweis: Weitere Informationen zum Installieren der Komponente für die Betriebssystem-Verteilung und die Profilmigration auf dem Core Server sowie zum Konfigurieren der Betriebssystem-Verteilungs- und Profilmigrationsumgebung finden Sie im *LANDesk Management Suite Installations- und Verteilungshandbuch*.

In diesem Kapitel erfahren Sie mehr über:

Betriebssystem-Verteilung

- Übersicht über die Betriebssystem-Verteilung
- Richtlinien für Betriebssystemabbilder
- Anpassen von Abbildern mit Sysprep und dem Installations-Manager
- Agentbasierte Bereitstellung
- Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Ändern von Skripts
- Multicasting für Betriebssystemabbilder
- Anzeigen von Abbildstatusberichten
- PXE-basierte Bereitstellung
- Verwenden von PXE-Repräsentanten
- Starten von Clients mit PXE
- Konfigurieren der Eingabeaufforderung für den PXE-Start
- Verwenden von "Von LANDesk gesteuertes Starten"
- Verwenden des PXE-DOS-Menüs
- Verwenden der PXE-Haltewarteschlange

Profilmigration

- Übersicht über die Profilmigration
- Profilinhalt
- Erstellen von Sammlungen
- Migrieren von Benutzerkonten

- Migrieren von Anwendungseinstellungen, Vorlagen und verknüpften Dateien
- Migrieren von Desktop(PC)-Einstellungen
- Migrieren von Dateien und Ordnern
- Erstellen von Dateiregeln
- Erstellen von Migrationsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Erstellen von benutzerinitiierten Profilmigrationspaketen
- Ausführen von benutzerinitiierten Profilmigrationspaketen

Übersicht über die Betriebssystem-Verteilung

In LANDesk Betriebssystem-Verteilung (OSD) gibt es zwei Methoden, Betriebssystemabbilder für Clients im Netzwerk bereitzustellen:

- **Agenten-basierte Bereitstellung:**Abbilder werden mit dem Windows-Betriebssystem des Clients und den installierten LANDesk-Agenten bereitgestellt. Weitere Informationen finden Sie unter "Agenten-basierte Bereitstellung" weiter unten in diesem Kapitel.
- **PXE-basierte Bereitstellung:**Ermöglicht das Erstellen von Abbildern für Clients mit leeren Festplatten oder nicht funktionsfähigen Betriebssystemen. Bei Verwendung von Lightweight .NET PXE-Repräsentanten wird nicht in jedem Subnetz ein dedizierter PXE-Server benötigt. Weitere Informationen finden Sie unter "PXE-basierte Bereitstellung" weiter unten in diesem Kapitel.

Wenn Sie zum Erstellen von Abbildern das Microsoft-Dienstprogramm Sysprep verwenden, werden mit der Betriebssystem-Verteilung angepasste SYSPREP.INF-Dateien erstellt und in die Abbilder der einzelnen Clients eingefügt. Auf diese Weise werden der Windows-Computername, die Domäneninformationen usw. aus der Core-Datenbank angepasst.

Die Betriebssystem-Verteilung enthält ein integriertes Abbildverarbeitungstool, mit dem Abbilder erstellt werden können. Darüber hinaus werden Abbildverarbeitungstools von anderen Herstellern unterstützt, die Sie u. U. bereits verwenden, z. B. Symantec Ghost* und PowerQuest DeployCenter*.

WARNUNG: Die Betriebssystem-Verteilung (Abbildverarbeitung) sollte mit größter Vorsicht eingesetzt werden. Bei der Betriebssystem-Verteilung werden alle Daten von der Festplatte eines Clients gelöscht. Anschließend wird ein neues Betriebssystem installiert. Es besteht das Risiko, dass wichtige Daten verloren gehen, wenn die Betriebssystem-Verteilung nicht genau entsprechend den Anweisungen in diesem Dokument ausgeführt wird oder wenn schlecht implementierte Abbilder verwendet werden. Bevor Sie eine Betriebssystem-Verteilung durchführen, sollten Sie alle Daten sichern, damit verloren gegangene Daten wiederhergestellt werden können.

Schritte bei der Betriebssystem-Verteilung

Gehen Sie beim Planen und Implementieren einer Betriebssystem-Verteilung wie folgt vor:

1. (Optional) Führen Sie den Installations-Manager von Microsoft und das Dienstprogramm Sysprep auf dem Client aus, dessen Abbild erfasst werden soll.
2. Erstellen Sie ein Abbilderfassungsskript mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten.
3. Planen Sie mit dem Management Suite-Werkzeug "Geplante Tasks" einen Task, mit der das Abbilderfassungsskript auf dem Client ausgeführt wird, dessen Abbild erfasst werden soll. (Im Fenster "Status des benutzerdefinierten Auftrags" wird angezeigt, ob diese Task erfolgreich war oder gescheitert ist.)

4. Erstellen Sie ein Abbildbereitstellungsskript mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten.
5. Planen Sie mit "Geplante Tasks" einen Task, mit dem das Abbildbereitstellungsskript auf den Ziel-Clients ausgeführt wird, auf denen das Abbild bereitgestellt werden soll.
6. Ziel-Clients, auf denen ein Windows-Betriebssystem und LANDesk-Agenten ausgeführt werden, führen den Abbildbereitstellungsauftrag zum geplanten Zeitpunkt aus (agentbasierte Bereitstellung).
7. PXE-fähige Ziel-Clients führen den Abbildbereitstellungsauftrag aus, wenn sie das nächste Mal gestartet werden (PXE-basierte Bereitstellung).

Ausführliche Informationen zu den einzelnen Schritten finden Sie in den betreffenden Abschnitten unten.

Richtlinien für Betriebssystemabbilder

Sie können Betriebssystemabbilder mit dem LANDesk-Abbildverarbeitungstool oder anderen Abbildverarbeitungstools erstellen. Wenn Sie den Betriebssystem-Verteilung/Migrationstasks-Assistenten ausführen, um ein Abbildverarbeitungsskript zu erstellen, werden Sie aufgefordert, den Abbildtyp und das Abbildverarbeitungstool anzugeben. Der Assistent erstellt automatisch Befehlszeilen für das LANDesk-Abbildverarbeitungstool, Symantec Ghost 7.5 und PowerQuest DeployCenter 5.01.1.

Hinweis: Wenn Sie die Komponente für die Betriebssystem-Verteilung und die Profilmigration installieren, werden automatisch Dateien für das LANDesk-Abbildverarbeitungstool auf dem Core Server installiert. Wenn Sie das LANDesk-Abbildverarbeitungstool von einem anderen Ort ausführen möchten, müssen Sie die folgenden vier Dateien kopieren: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT und BACKALL.BAT.

Wenn Sie mit einem anderen Abbildverarbeitungstool arbeiten, können Sie die Befehlszeile dafür am Ende des Assistenten angeben. Bei Angabe einer benutzerdefinierten Befehlszeile fügt der Assistent diese Zeile an der richtigen Stelle im Skript ein, und Sie müssen das Skript nicht manuell bearbeiten.

Abbilddateinamen

Weisen Sie den Abbildern eindeutige Dateinamen zu. Wenn Sie gleichzeitig verschiedene Abbilder mit demselben Dateinamen im selben Subnetz bereitstellen, können Probleme auftreten. Je nachdem, welche Namen den Abbilddateien vom Abbildverarbeitungstool zugewiesen werden (z. B. Ghost-Multidateiabbilder), besitzt der Dateiname u. U. nur fünf eindeutige Zeichen, sobald er in ein DOS 8.3-Namensformat konvertiert wurde.

Die Betriebssystem-Verteilung verwendet für Abbildnamen die ersten acht Zeichen des Windows-Computernamens, auf dem das Abbild erstellt wurde. Wenn das Abbild aus mehreren Abbilddateien besteht, verwendet das Abbildverarbeitungstool u. U. nur die ersten fünf Zeichen. Werden Abbilder von mehreren Clients erfasst, gibt es zwei Möglichkeiten sicherzustellen, dass die Abbilder eindeutige Namen aufweisen:

- Erstellen Sie ein Client-Abbild nach dem anderen, und benennen Sie die Abbilder unmittelbar nach ihrer Erstellung um.
- Stellen Sie vor Ausführung des Auftrags sicher, dass die ersten acht Zeichen (oder fünf Zeichen bei Multidateiabbildern) der Windows-Computernamen des Abbildes eindeutig sind.

Spezifikationen und Anforderungen für Abbilddateien

Unabhängig vom verwendeten Abbildverarbeitungstool darf die Größe des komprimierten Abbildes aufgrund von DOS-Größenbeschränkungen und Einschränkungen des Tools nicht größer als 2 GB sein.

Die Betriebssystem-Verteilung unterstützt NTFS-, FAT- und FAT32-Dateisysteme.

LANDesk-Agenten und -Abbilder

Die Abbilder sollten keine LANDesk-Agenten enthalten. Wenn Sie ein Sysprep-Abbild verwenden, installiert die Betriebssystem-Verteilung die LANDesk-Agenten, nachdem das Abbild wiederhergestellt wurde.

Wenn Nicht-Sysprep-Abbilder LANDesk-Agenten enthalten, müssen Sie die Datei LDISCAN.CFG aus dem Rootverzeichnis der Festplatte löschen, bevor Sie mit der Abbildverarbeitung beginnen. Außerdem müssen Sie den Schlüssel "Unique ID" unter HKLM/Software/Intel/LANDesk/Common API löschen. Andernfalls besitzen alle Clients, die das Abbild verwenden, denselben Core-Datenbankeintrag. Es gibt noch eine andere Möglichkeit: Wenn Nicht-Sysprep-Abbilder bereits LANDesk-Agenten besitzen, können Sie die Option**Doppelte Kennungen ablehnen** im Dialogfeld **Doppelte Gerätekennung** aktivieren (**Konfigurieren | Dienste | Inventar | ID duplizieren**).

Partitionen und Abbilder

Wenn die Betriebssystem-Verteilung ein Abbild auf einem Ziel-Client wiederherstellt, werden standardmäßig alle bereits vorhandenen Partitionen auf diesem Client gelöscht.

Das LANDesk-Abbildverarbeitungstool unterstützt Abbildungen mit einzelnen oder mehreren Partitionen (bis zu vier).

Nicht-Windows-Abbilder

Mit der Betriebssystem-Verteilung können Sie fast jedes Abbild bereitstellen, das vom Abbildverarbeitungstool unterstützt wird, nicht nur Windows-basierte Abbilder. Beim Bereitstellen eines nicht mit Windows oder nicht mit Sysprep vorbereiteten Abbildes darf die Option **Abbild ist mit Sysprep vorbereitet** auf der Seite **Bildverarbeitungs-Task konfigurieren** des Betriebssystem-Verteilung/Migrationstasks-Assistenten nicht aktiviert sein.

Anpassen von Abbildern mit Sysprep und dem Installations-Manager

Sie können die Microsoft-Dienstprogramme Installations-Manager und Sysprep für die Bereitstellung von Windows 2000- und Windows XP-Abbildern verwenden. Sysprep passt eine Windows-Installation so an, dass beim Neustart des Betriebssystems nach einer Antwortdatei (SYSPREP.INF) gesucht wird und sich das Betriebssystem selbst für den neuen Client konfiguriert.Der Installations-Manager erstellt die SYSPREP.INF-Antwortdatei, die Sysprep verwendet.

Bevor Sie Betriebssystem-Verteilungsskripts erstellen, sollten Sie den Installations-Manager von Microsoft (SETUPMGR.EXE) ausführen und eine SYSPREP.INF-Antwortdatei für die bereitgestellten Abbilder erstellen. Sie können diese Datei anschließend als Grundlage für erstellte Betriebssystem-Verteilungsskripts verwenden, indem Sie die Option **Vorhandene SYSPREP.INF-Datei als Vorlage verwenden** auf der Assistentenseite **Sysprep-Dateiinformationen angeben** auswählen. Alle Einstellungen, die Sie im Assistenten für Betriebssystem-Verteilungsskripts eingeben, überschreiben die entsprechenden Optionen in der SYSPREP.INF-Vorlagendatei.

Wenn Sie Sysprep für Windows 2000/XP-Abbilder verwenden, kann die Betriebssystem-Verteilung eine Core-Datenbankabfrage nach den von Ihnen bereitgestellten Clients erstellen und bestimmte Benutzereinstellungen migrieren, z. B.:

- Windows-Computername
- Management Suite-GUID (die eindeutige Kennung, mit der Management Suite Clients in der Core-Datenbank identifiziert)

Sie können auch diese Optionen global für bereitgestellte Abbilder festlegen:

- Zeitzone
- Datenträgerlizenzschlüssel
- Registrierter Name und Organisation
- Arbeitsgruppe/Domäne/LDAP-Organisationseinheit

Die Betriebssystem-Verteilung verwendet Informationen aus der Core-Datenbank und aus dem Abbildbereitstellungsskript zum Erstellen einer benutzerdefinierten SYSPREP.INF-Datei für jeden abgebildeten Client. Anschließend wird die SYSPREP.INF-Datei in die einzelnen Client-Abbilder eingefügt.

Erstellen eines Sysprep-Abbildes

So erstellen Sie ein Abbild, das Sysprep verwendet

1. Um den Client, dessen Abbild erfasst werden soll, auf die Abbildverarbeitung vorzubereiten, nehmen Sie die erforderlichen Konfigurationsänderungen oder Anpassungen vor.
2. Erstellen Sie einen Ordner c:\sysprep im Rootverzeichnis der Client-Festplatte.

3. Wechseln Sie auf einer Windows 2000- oder Windows XP-Installations-CD zum Verzeichnis \Support\Tools\DEPLOY.CAB, und kopieren Sie **SYSPREP.EXE** und **SETUPCL.EXE** in den erstellten sysprep-Ordner.
4. Öffnen Sie eine DOS-Eingabeaufforderung, und wechseln Sie zum sysprep-Ordner. Führen Sie Sysprep aus. Wenn Sie nicht die Neustartoption verwenden, müssen Sie den Client über das Startmenü herunterfahren, sobald Sie zum Herunterfahren aufgefordert werden.
5. Starten Sie im DOS-Modus, und führen Sie das Abbildverarbeitungstool manuell aus.

Weitere Informationen zum Installations-Manager und zu Sysprep

Auf der Microsoft-Website finden Sie die offizielle Dokumentation zum Installations-Manager und zum Sysprep-Dienstprogramm. Sysprep umfasst zahlreiche andere hilfreiche Funktionen, die nicht in diesem Dokument beschrieben werden.

Agentbasierte Bereitstellung

Mit Hilfe der agentbasierten Bereitstellungsmethode können Sie Betriebssystemabbilder für Clients bereitstellen, auf denen Windows 98, Windows 2000 oder Windows XP ausgeführt wird.

Informationen zu anderen Methoden der Abbildbereitstellung finden Sie unter "PXE-basierte Bereitstellung" weiter unten in diesem Kapitel.

Voraussetzungen

Wenn Sie Abbilder nicht mit Hilfe von PXE bereitstellen, müssen Clients die folgenden Kriterien erfüllen:

- Sie müssen in der Core-Datenbank enthalten sein, wenn Sie Multiprozessorabbilder besitzen.
- Die CBA-, Enhanced Software Distribution- und Inventaragenten müssen geladen sein. Die Betriebssystem-Verteilung verwendet den Enhanced Software Distribution-Agenten zum Verteilen von Abbildern. Wenn Sie Multicasting verwenden möchten, muss der Targeted Multicasting-Agent ebenfalls geladen sein.

Was passiert bei einer agentbasierten Bereitstellung?

1. Management Suite stellt eine Verbindung zum Client her und führt alle Vorkonfigurationsbefehle aus, die Sie im Abbildbereitstellungsskript angegeben haben.
2. Die Betriebssystem-Verteilung verwendet den Enhanced Software Distribution-Agenten, um eine virtuelle Startpartitionsdatei an den Client zu verteilen. Außerdem wird der Startsektor bearbeitet, damit von dieser Datei gestartet wird. Dann wird der Client neu gestartet.
3. Der Client startet im DOS-Modus, ermittelt und lädt einen Netzwerktreiber, bevor er die Abbilddatei vom Abbildserver abruft und installiert.

   Bei Nicht-Sysprep-Abbildern startet der Client nach Abschluss der Abbildverarbeitung neu. Die Betriebssystem-Verteilung betrachtet den Auftrag nach diesem Neustart als abgeschlossen.

   Bei Sysprep-Abbildern wird die agentbasierte Bereitstellung folgendermaßen fortgesetzt:

4. Vor dem Neustart und dem Laden des Abbildes ersetzt der DOS-Agent SYSPREP.INF durch eine für diesen Client angepasste Datei.
5. Der abgebildete Client wird gestartet und passt sich entsprechend den Einstellungen in der SYSPREP.INF-Datei an.
6. Alle Befehle, die nach dem Abbilden im Abbildbereitstellungsskript angegeben wurden, werden über den Registrierungsschlüssel "RunOnce" ausgeführt.
7. Die Betriebssystem-Verteilung führt WSCFG32.EXE mit der Client-Standardkonfiguration aus, um die LANDesk-Agenten neu zu installieren.

Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten

In der Betriebssystem-Verteilung von Management Suite gibt es den Betriebssystem-Verteilung/Migrationstasks-Assistenten, mit dem Sie sowohl Abbildverarbeitungsskripts (Abbilderfassung und -bereitstellung) als auch Profilmigrationsskripts erstellen können. Alle LANDesk Management Suite-Skripts werden mit dem Werkzeug "Skripte verwalten" (**Extras | Skripte verwalten**) verwaltet.

Ausführliche Beschreibungen der einzelnen Seiten der Assistentenoberfläche finden Sie im Abschnitt "Hilfe zum Betriebssystem-Verteilung/Migrationstasks-Assistenten" in Anhang B.

Mit dem Assistenten können Sie Skripts erstellen, die folgende Tasks ausführen:

- **Abbild erfassen:** Erstellt ein Skript, das ein Betriebssystemabbild von einem Client erfasst und speichert. Abbilder können mit Hilfe des integrierten LANDesk-Abbildverarbeitungstools erfasst werden, das mit Management Suite installiert wird, oder mit einem Tool eines anderen Herstellers, z. B. Ghost oder PowerQuest.
- **Profil erfassen:** Erstellt ein Skript, das die einem Client eigenen Benutzereinstellungen, Anwendungs- und Desktopeinstellungen sowie Dateien erfasst. Mit dieser Option können Sie auch auf das Dialogfeld "Sammlungsmanager" zugreifen, um ein benutzerinitiiertes Profilmigrationspaket zu erstellen, das lokal auf einzelnen Clients ausgeführt werden kann.
- **Abbild bereitstellen:** Erstellt ein Skript, das ein zuvor erfasstes OS-Abbild für Ziel-Clients bereitstellt.
- **Abbild bereitstellen (mit Profilerfassung und -wiederherstellung):** Erstellt ein Skript, das einen umfassenden Bereitstellungs- und Migrationsauftrag ausführt (Erfassen von Profildaten, Bereitstellen eines Betriebssystem-Abbilds und Wiederherstellen des Profils).
- **Profil wiederherstellen:** Erstellt ein Skript, das zuvor erfasste Profildaten auf Ziel-Clients wiederherstellt (Benutzereinstellungen, Anwendungs- und Desktopeinstellungen sowie Dateien).
- **Generische DOS-Tasks:** Erstellt ein Skript, das auf Clients DOS-Befehle ausführt (einschließlich Starten von Anwendungen).

Sobald Sie ein Skript erstellt haben, können Sie über "Geplante Tasks" seine Ausführung auf Clients planen.

Erstellen von benutzerinitiierten Profilmigrationspaketen
Im Betriebssystem-Verteilung/Migrationstasks-Assistenten können Sie auch auf das Dialogfeld "Sammlungsmanager" zugreifen, in dem Sie ein benutzerinitiiertes Profilmigrationspaket (eine selbstextrahierende ausführbare Datei) erstellen können, das für die benutzerinitiierte Profilmigration an Clients verteilt und darauf ausgeführt werden kann. Weitere Informationen finden Sie unter "Erstellen von benutzerinitiierten Profilmigrationspaketen" weiter unten in diesem Kapitel.

Wenn Sie ein Abbild für PXE-fähige Clients bereitstellen, können Sie Abbildbereitstellungsskripts in das PXE-DOS-Startmenü einfügen. Dieses Menü ist DOS-basiert und wird beim PXE-Start auf dem Client angezeigt. Weitere Informationen finden Sie unter "Verwenden des PXE-DOS-Menüs" weiter unten in diesem Kapitel.

So führen Sie den Betriebssystem-Verteilung/Migrationstasks-Assistenten aus

1. Klicken Sie auf **Extras | Skripte verwalten**.
2. Klicken Sie im Fenster "Skripte verwalten" mit der rechten Maustaste auf **Alle OSD-/Profilmigrationsskripts**, anschließend klicken Sie im Kontextmenü auf **Neues OSD-/Profilmigrationsskript**, um den Assistenten zu öffnen. Oder klicken Sie im Fenster "Skripte verwalten" in der Symbolleiste auf die Schaltfläche **Neues OSD-/Profilmigrationsskript**.
3. Wählen Sie den zu erstellenden Skripttyp aus. Um die Online-Hilfe für die Optionen auf den Assistentenseiten aufzurufen, klicken Sie auf **Hilfe**.
4. Führen Sie die Schritte des Assistenten aus, bis Sie die letzte Seite erreicht haben. Klicken Sie auf **Fertigstellen**, um das Skript zu speichern und den Assistenten zu beenden. Sobald das Skript erstellt ist, wird es im Fenster "Skripte verwalten" in der Gruppe "Alle OSD-/Profilmigrationsskripts" angezeigt.

Administratoren (Benutzer mit LANDesk-Administratorrechten) können in der Gruppe "Benutzerskripts" Skripts in Untergruppen von Benutzern kopieren.

Weitere Hinweise zu Skripts

- Skriptnamen müssen den Windows-Dateinamenskonventionen entsprechen. Der Assistent verwendet den eingegebenen Skriptnamen als Dateinamen. Wenn Sie Zeichen verwenden, die in Windows-Dateinamen nicht zulässig sind, wird eine entsprechende Meldung ausgegeben.
- Alle Skripts werden auf dem Core Server im Verzeichnis \\<core>\LDMain\Scripts gespeichert. Wenn Sie mehrere Management Suite-Konsolen verwenden, werden die Skripts im Fenster "Skripte verwalten" der einzelnen Konsolen angezeigt.
- Auf den Assistentenseiten werden die Einstellungen des zuletzt erstellten Skripts wiederhergestellt. Wenn Sie den Skripttyp von einem Bildverarbeitungs-Task zu einem Profilmigrationstask oder einem DOS-Task ändern, löscht der Assistent die gespeicherten Einstellungen.

Info über die Skripts "Generische DOS-Tasks"

- DOS-Skripts starten die ausgewählten Ziel-Clients neu und führen die angegebenen Befehle aus. Diese Fernbefehle werden zeilenweise gesendet.
- DOS-Skripts werden von der virtuellen Startpartition ausgeführt und durchlaufen denselben Netzwerkerkennungsprozess wie normale Betriebssystem-Verteilungen.
- Mit der Option "Diesen Auftrag abbrechen, wenn ein Befehl fehlschlägt" wird die Ausführung angehalten, falls einer der Befehle eine DOS-Fehlerebene ungleich Null zurückgibt. Sie können den DOS-Task-Status im Fenster "Benutzerdefinierter Auftrag" oder in einem Bericht überprüfen.

- Weitere Informationen zu Skriptbefehlen finden Sie im Whitepaper "Using Custom Scripts" (Verwenden benutzerdefinierter Skripts) unter http://support.landesk.com.

Ändern von Skripts

Sie können Ihre Skripts jederzeit bearbeiten, entweder indem Sie den Assistenten neu öffnen und Änderungen vornehmen oder indem Sie das Skript direkt in seiner .INI-Datei bearbeiten und alle bestehenden Sysprep-Einstellungen in der zugehörigen .INF-Datei bearbeiten.

Hinweis: Bei DOS-Skripts dürfen ausschließlich Änderungen zwischen den Zeilen REMPINGx=DOS und REMEXECx=reboot.com vorgenommen werden. Die anderen Zeilen im Skript sind für die virtuellen Startpartitionsdateien und den Startprozess verantwortlich.

So bearbeiten Sie ein Skript über den Assistenten.

1. Klicken Sie auf **Extras | Skripte verwalten**.
2. Klicken Sie mit der rechten Maustaste auf das Skript, und klicken Sie im Kontextmenü auf **Bearbeiten** (oder doppelklicken Sie auf das Skript).
3. Gehen Sie Schritt für Schritt durch den Assistenten, und nehmen Sie die gewünschten Änderungen vor.

So bearbeiten Sie ein Skript über eine .INI-Datei

1. Klicken Sie auf **Extras | Skripte verwalten**.
2. Klicken Sie mit der rechten Maustaste auf das Skript, und klicken Sie auf **Erweiterte Bearbeitung**. Die .INI-Datei des Skripts wird im Editor geöffnet. Wenn es für dieses Skript Sysprep-Einstellungen gibt, wird die SYSPREP.INF-Datei ebenfalls im Editor geöffnet.
3. Nehmen Sie die Änderungen vor.
4. Speichern Sie die Datei(en).

Speicherort von .INI- und .INF-Dateien
.INI-Dateien werden im Verzeichnis \\<core>\LDMain\Scripts gespeichert. .INF-Dateien werden im Verzeichnis \\<core>\LDMain\LANDesk\Files gespeichert.

Multicasting für Betriebssystemabbilder

In diesem Abschnitt wird beschrieben, wie Abbilder mit der Targeted Multicasting-Technologie von LANDesk bereitgestellt werden. Targeted Multicasting ist langsamer als Einzelverteilungen. Multicasting benötigt weniger Bandbreite und legt das Abbild auf der Festplatte des Ziel-Clients bereit. Bei vier oder mehr Clients lohnt sich der Einsatz von Multicasting jedoch, weil dann genügend Bandbreite eingespart wird.

Targeted Multicasting unterstützt nur Abbilder mit einzelnen Partitionen. Wenn Sie Targeted Multicasting mit der Betriebssystem-Verteilung verwenden, können Abbilder bis zu zehn Dateien umfassen.

Beim Multicasting von Abbildern wird die Abbilddatei im Zwischenspeicher des Clients abgelegt, bevor sie wiederhergestellt wird. Auf der Festplatte muss genügend Speicherplatz für die Abbilddatei und die wiederhergestellten Dateien vorhanden sein.

Bevor Sie Targeted Multicasting mit der Betriebssystem-Verteilung verwenden können, müssen Sie sicherstellen, dass das Subnetz, an das die Abbilddateien verteilt/bereitgestellt werden sollen, Targeted Multicasting-Komponenten enthält. Um Targeted Multicasting verwenden zu können, müssen auf den Clients Agenten von Management Suite 6.62 oder höher und im Subnetz ein Multicast-Domänenrepräsentant von LANDesk Management Suite 6.62 oder höher installiert sein.

Wenn Sie Dateien mit Hilfe von Multicasting an ein Subnetz verteilen möchten, das keinen Multicast-Domänenrepräsentanten besitzt, wird die Bereitstellung zwar gestartet, sie kann jedoch nicht abgeschlossen werden. Sie müssen eine Startdiskette für die Betriebssystem-Verteilung erstellen. Weitere Informationen finden Sie unter "Erstellen einer OSD-Bootdiskette" in Anhang B.

Wenn die Router UDP-Broadcasts weiterleiten und es im Subnetz, das das verteilte Abbild erhält, Windows-Clients gibt, die als Multicast-Domänenrepräsentant fungieren können, kann Targeted Multicasting verwendet werden, ohne dass Multicast-Domänenrepräsentanten angegeben werden müssen. Wenn die Router keine UDP-Broadcasts weiterleiten, müssen Sie die Multicast-Domänenrepräsentanten manuell für jedes Subnetz auswählen. Dabei müssen Sie darauf achten, dass die ausgewählten Repräsentanten nicht zu den Clients gehören, an die Abbilder verteilt werden.

Sie können manuell festlegen, welche Clients als Multicastdomänenrepräsentanten verwendet werden sollen, indem Sie Clients zur Gruppe **Konfiguration > Multicastdomänenrepräsentanten** in der Konsole hinzufügen.

Sie dürfen keine Abbilder von Multicast-Domänenrepräsentanten in einem Subnetz erstellen, weil diese Abbildverarbeitung fehlschlägt und die Clients anschließend nicht mehr funktionsfähig sind.

Um die Multicasts zu reduzieren, ändern Sie die Option **Mindestanzahl der Millisekunden zwischen Paketübertragungen** im Dialogfeld **Erweiterte Multicast-Optionen konfigurieren** des Betriebssystem-Verteilung/Migrationstasks-Assistenten.

WARNUNG: Wenn die Multicasting-Umgebung nicht richtig konfiguriert ist und Targeted Multicasting fehlschlägt, kann es sein, dass keiner der Ziel-Clients gestartet werden kann, sofern nicht die oben beschriebenen Anweisungen befolgt werden.

Anzeigen von Abbildstatusberichten

Der abgebildete Client sendet Statusaktualisierungen an den Core Server. Sie können den Status im Fenster "Benutzerdefinierter Auftrag" oder in einem Bericht überwachen. Wenn die Betriebssystem-Verteilung Abbildverarbeitungsbefehle an Clients sendet, werden die Befehle im Fenster "Benutzerdefinierter Auftrag" angezeigt. Abgebildete Clients senden Statusaktualisierungen für jeden gesendeten Skriptbefehl. Falls die Abbildbereitstellung fehlschlägt, wird der fehlgeschlagene Befehl angezeigt.

Allgemeine Gründe für das Fehlschlagen der Abbildverarbeitung:

- Beschädigte Partition
- Probleme, die vom Abbildverarbeitungstool nicht bewältigt werden können
- Die Autoerkennung für Netzwerkadapter kann keinen Netzwerkadapter finden
- Der angegebene Netzwerkadapter, der nicht gefunden werden konnte, funktioniert nicht (Wenn der angegebene Netzwerkadaptertreiber nicht geladen wird, hält der Client bei der DOS-Eingabeaufforderung an. Sie müssen ihn dann manuell neu starten.)

Die Betriebssystem-Verteilung erstellt einen Statusbericht für jeden Auftrag und zeigt darin, ob der Auftrag auf den Ziel-Clients erfolgreich ausgeführt wurde oder nicht.

So zeigen Sie einen Statusbericht an

1. Klicken Sie auf **Extras | Berichte | Alle LDMS-Berichte**.
2. Wählen Sie den Bericht **OS-Verteilungserfolgsrate** aus.
3. Wählen Sie in der Liste der Protokolldateien die Datei für den Auftrag aus, der angezeigt werden soll.
4. Klicken Sie auf **Ausführen**.

Am Anfang der Berichte werden die Aufträge angezeigt, die für einzelne Clients fehlgeschlagen sind. Die Berichte enthalten außerdem Einzelheiten zu den Aufträgen, z. B.:

- **Rechnername:** Bei Clients, die bereits in der Core-Datenbank enthalten sind, ist dies der dem Client zugewiesene Gerätename. Bei Clients, die über PXE gestartet werden und noch nicht vom Inventarscanner erfasst wurden, wird eine MAC-Adresse als Rechnername verwendet. Sie können eine .CSV-Datei verwenden, um MAC-Adressen in die Core-Datenbank zu importieren. Weitere Informationen finden Sie unter "Verwenden von CSVIMPORT.EXE zum Importieren von Inventardaten" in Anhang B.
- **Status:** Auftragsstatus, fehlgeschlagen oder OK.
- **Dauer:** Zeit, die zur Ausführung der einzelnen Befehle benötigt wurde.
- **Befehle:** Jeder Befehl, der als Teil des Skripts ausgeführt wurde. Wenn ein Auftrag fehlschlägt, wird in dieser Spalte angezeigt, welcher Befehl dafür verantwortlich ist.

PXE-basierte Bereitstellung

Die Betriebssystem-Verteilung unterstützt PXE-Starts und die Abbildbereitstellung. Die PXE-basierte Bereitstellung ist (neben der agentbasierten Bereitstellung) eine weitere Methode für die automatisierte Fernabbildverarbeitung von Clients im Netzwerk. Mit PXE-Unterstützung können Sie sowohl neue als auch vorhandene PXE-fähige Clients starten und entweder über ein benutzerdefiniertes PXE-DOS-Startmenü ein Betriebssystem-Verteilungsskript auf dem Client ausführen oder Clients in die Core-Datenbank scannen und anschließend mit "Geplante Tasks" einen Abbildbereitstellungsauftrag planen.

Die PXE-basierte Bereitstellung bietet in verschiedenen Situationen eine schnelle und einfache Möglichkeit, Clients abzubilden. Beispiele:

- Anfängliche Bereitstellung neuer Clients
- Abbilden von Clients in einer Test- oder Schulungsumgebung
- Erneutes Abbilden von beschädigten Clients

Management Suite enthält verschiedene Optionen für die Verwendung von PXE zum Bereitstellen von Betriebssystemabbildern. Weitere Informationen finden Sie unter "Erläuterungen zu den PXE-Startoptionen" weiter unten in diesem Kapitel.

Grundlagen von PXE-Protokollen

PXE (Preboot Execution Environment) ist ein dem Industriestandard entsprechendes Netzwerkprotokoll, mit dem Clients über das Netzwerk gestartet und abgebildet werden können. Dazu wird eine ausführbare Abbilddatei von einem Abbildserver heruntergeladen und installiert, bevor der Client von der lokalen Festplatte gestartet wird. Auf einem PXE-fähigen Client wird das PXE-Protokoll entweder vom Flash-Speicher bzw. -ROM des Netzwerkadapters oder vom System-BIOS geladen.

PXE verwendet folgende Kommunikationsstandards: DHCP (Dynamic Host Configuration Protocol), TFTP (Trivial File Transfer Protocol) und MTFTP (Multicast Trivial File Transfer Protocol).

Beim Start eines PXE-fähigen Clients wird eine DHCP-Erkennungsanforderung ausgesendet. Wenn ein DHCP-Server erkannt wird, der PXE implementiert, weist der Server dem Client eine IP-Adresse zu und sendet Informationen zu verfügbaren PXE-Startservern. Wenn der DHCP-Erkennungsprozess abgeschlossen ist, kontaktiert der Client den PXE-Server und lädt über TFTP eine Abbilddatei herunter. Anschließend wird das Abbildverarbeitungsskript ausgeführt, mit dem das Betriebssystemabbild vom Abbildverarbeitungsserver auf den Client geladen wird. Mit Management Suite wird in einem Betriebssystem-Verteilungsskript auf die Abbilddatei verwiesen.

Weitere Informationen zu PXE und den zugrunde liegenden Technologien und Funktionen finden Sie in der PXE-Spezifikation v2.1 unter http://www.intel.com/labs/manage/wfm/wfmspecs.htm.

Verwenden von PXE-Repräsentanten

Die PXE-Unterstützungssoftware wird im Rahmen der Standardinstallation der Betriebssystem-Verteilung auf dem Core Server installiert. Um PXE-Unterstützung zu aktivieren, müssen Sie jedoch zunächst einen PXE-Repräsentanten in jedem Subnetz des Netzwerks bereitstellen, das PXE-Unterstützung bieten soll. PXE-Repräsentanten sorgen für Skalierbarkeit im Netzwerk, weil Betriebssystemabbilder an Clients in ihren jeweiligen Subnetzen bereitgestellt werden.

Die Clients in den Subnetzen verwenden normale PXE-Abfragen und Dateiübertragungsmethoden, um mit dem vorhandenen PXE-Repräsentanten zu kommunizieren, der wiederum mit Hilfe von Webdiensten (HTTP) mit dem Core Server kommuniziert.

Deaktivieren von anderen PXE-Servern
Falls derzeit *irgendein* anderer PXE-Server im Netzwerk ausgeführt wird, müssen Sie ihn zuerst deaktivieren, um die LANDesk-PXE-Unterstützung nutzen zu können.

Bereitstellen von PXE-Repräsentanten

Sie müssen mindestens einen PXE-Repräsentanten im Netzwerk bereitstellen und mindestens einen weiteren PXE-Repräsentanten in den einzelnen Subnetzen, für die PXE-Startunterstützung gewährleistet werden soll. Um einen PXE-Repräsentanten einzurichten, müssen Sie das Skript "PXE-Repräsentantenverteilung" auf dem ausgewählten Client ausführen. Dieses vordefinierte Skript ist im Dialogfeld "Skript planen" verfügbar (**Extras | Geplante Tasks |** und in der Symbolleiste auf die Schaltfläche **Skript planen** klicken).

Um einen Lastenausgleich sicherzustellen, können in einem Subnetz mehrere PXE-Repräsentanten vorhanden sein. In diesem Fall wird der erste PXE-Repräsentant, der auf eine Clientanforderung antwortet, für die Kommunikation mit dem Core Server verwendet.

Hinweis: Auf dem Core Server sollte *kein* PXE-Repräsentant bereitgestellt werden.

Der als PXE-Repräsentant ausgewählte Client muss keine speziellen Hardwareanforderungen erfüllen. Es gelten jedoch folgende Softwareanforderungen:

- **Betriebssystem:** Windows NT 4, Windows 2000 oder Windows XP.

  Bei Windows NT und 2000 müssen Sie sicherstellen, dass der Microsoft-MSI-Dienst ausgeführt wird (XP umfasst MSI standardmäßig). Wenn der neueste Service Pack für das verwendete Betriebssystem installiert ist, wird der MSI-Dienst im Normalfall ausgeführt. Andernfalls können Sie ihn folgendermaßen über die Management Suite-Konsole auf dem PXE-Repräsentanten bereitstellen: Klicken Sie auf **Extras | Geplante Tasks** und in der Symbolleiste auf die Schaltfläche **Skript planen**. Wählen Sie den Task **MSI-Dienst-Verteilung** aus, klicken Sie auf **OK**, ziehen Sie den bzw. die Ziel-Clients in das Fenster, und klicken Sie auf die Schaltfläche **Startzeit festlegen**, um den MSI-Dienst bereitzustellen.

- **Installierte LANDesk-Agenten:** Enhanced Software Distribution-Agent und Inventarscanneragent. Weitere Informationen zum Installieren von Agenten finden Sie im *Installations- und Verteilungshandbuch*.

So stellen Sie einen PXE-Repräsentanten bereit

1. Klicken Sie auf **Extras | Geplante Tasks** und anschließend in der Symbolleiste auf die Schaltfläche **Skript planen**.
2. Wählen Sie das Skript **PXE-Repräsentantenverteilung** in der Liste aus, und klicken Sie auf **OK**.
3. Wählen Sie in der Netzwerkansicht der Konsole die Ziel-Clients aus, auf denen der PXE-Repräsentant installiert werden soll.
4. Fügen Sie die ausgewählten Clients mittels Ziehen und Ablegen in die Rechnerliste im Fenster "Geplante Tasks" ein.
5. Klicken Sie in der Symbolleiste auf die Schaltfläche **Startzeit festlegen**, um das Skript sofort oder zu einem späteren Zeitpunkt auszuführen.

Aktualisieren von PXE-Repräsentanten
Wenn Sie die Einstellungen für die PXE-Startoption (unter **Konfigurieren | Dienste | Betriebssystem-Verteilung**) ändern, müssen Sie alle PXE-Repräsentanten aktualisieren, indem Sie das Skript "PXE-Repräsentantenverteilung" erneut ausführen, damit die Änderungen für die PXE-Repräsentanten der einzelnen Subnetze übernommen werden. Die erneute Ausführung des Skripts ist jedoch nicht erforderlich, wenn Sie die PXE-Proxies nur aus der Liste "Verfügbare Proxies" in die Liste "Haltewarteschlangen-Proxies" verschieben. Weitere Informationen zur PXE-Haltewarteschlange finden Sie unter "Verwenden der PXE-Haltewarteschlange" weiter unten in diesem Kapitel.

So aktualisieren oder entfernen Sie einen PXE-Repräsentanten

1. Klicken Sie auf **Extras | Geplante Tasks** und anschließend in der Symbolleiste auf die Schaltfläche **Skript planen**.
2. Um einen PXE-Repräsentanten zu aktualisieren, wählen Sie das Skript **PXE-Repräsentantenverteilung** in der Liste aus, und klicken Sie auf **OK**.
3. Um einen PXE-Repräsentanten zu entfernen, wählen Sie das Skript **PXE-Repräsentantenentfernung** in der Liste aus, und klicken Sie auf **OK**.
4. Ziehen Sie die Ziel-Clients in das Fenster "Geplante Tasks", und legen Sie eine Uhrzeit für die Ausführung des Task fest.

Starten von Clients mit PXE

Wenn ein PXE-fähiger Client gestartet wird, passiert Folgendes:

1. Der PXE-fähige Client sendet eine Abfrage für PXE-Dienste aus, die auf einem PXE-Repräsentanten im Netzwerk ausgeführt werden.
2. Wenn ein PXE-Repräsentant im Subnetz vorhanden ist, antwortet er und weist den Client an, den Startvorgang mit PXE fortzusetzen.
3. Auf dem Client wird eine PXE-Startsitzung initiiert, und die Eingabeaufforderung für den PXE-Start wird angezeigt. Die Standardeingabeaufforderung lautet "Drücken Sie F8, um das Menü anzuzeigen." und wird vier Sekunden lang angezeigt. (Sie können die Einstellungen für diese Eingabeaufforderung auf dem Register **Konfigurieren | Management Suite-Dienste | Betriebssystem-Verteilung** ändern.)
4. Wenn die Taste **F8** vor Ablauf des Zeitintervalls gedrückt wird, wird ein vorläufiges PXE-Startmenü angezeigt, in dem Sie folgende Startoptionen auswählen können:

   - **Lokales Starten:** Der Client wird über die lokale Festplatte gestartet. Wenn kein Betriebssystem vorhanden ist, wird eine Fehlermeldung ausgegeben.
   - **Von LANDesk gesteuertes Starten:** Der Client wird in die Netzwerkansicht der Konsole eingefügt (die MAC-Adresse des Clients wird angezeigt), wo Sie die Ausführung eines Betriebssystem-Verteilungsskripts auf dem Client planen können.
   - **LANDesk-Startmenü:**Der Client zeigt das Startmenü an, das Sie mit dem Werkzeug "PXE-Startmenü" erstellt haben. Sie können ein Betriebssystem-Verteilungsskript auswählen und auf dem Client ausführen. Weitere Informationen finden Sie unter "Verwenden des PXE-Startmenüs" weiter unten in diesem Kapitel.

5. Wenn die Taste **F8** nicht vor Ablauf des Zeitintervalls gedrückt wird, verwendet der Client die standardmäßige Startoption. Die standardmäßige Startoption hängt von folgenden Bedingungen ab:

   - Wenn der Client einen geplanten Abbildverarbeitungsauftrag für sich in der Core-Datenbank ermittelt (entweder ein fehlgeschlagener oder anstehender Auftrag), wird **Von LANDesk gesteuertes Starten** als standardmäßige Startoption verwendet.
   - Wenn der Client *keinen* Abbildverarbeitungsauftrag für sich ermittelt, wird standardmäßig **Lokales Starten** verwendet.
   - **PXE-DOS-Menü** wird nie als standardmäßige Startoption verwendet.

6. Das geplante Betriebssystem-Verteilungsskript wird auf dem Client ausgeführt.

Erläuterungen zu den PXE-Startoptionen

Dieser Abschnitt enthält Informationen zum Konfigurieren der Eingabeaufforderung für den PXE-Start und zur Verwendung der folgenden PXE-Startoptionen:

- Von LANDesk gesteuertes Starten
- PXE-Startmenü
- PXE-Haltewarteschlange

Konfigurieren der Eingabeaufforderung für den PXE-Start

Sie können das Verhalten der Eingabeaufforderung für den PXE-Start steuern, die beim Versuch eines PXE-Starts durch den Client angezeigt wird.

Beim Starten eines PXE-fähigen Clients versucht eine DHCP-Anforderung eine PXE-Sitzung zu initiieren, indem sie nach einem Server (oder Proxy) sucht, auf dem die PXE-Dienstesoftware (PXE- und MTFTP-Dienste) ausgeführt wird. Wenn der Client einen PXE-Server entdeckt, wird auf dem Client einige Sekunden die Eingabeaufforderung für den PXE-Start angezeigt. Wenn Sie vor Ablauf des Zeitintervalls die Funktionstaste F8 drücken, können Sie auf das PXE-Startmenü zugreifen und ein Betriebssystemabbild auswählen, um es auf dem Client bereitzustellen.

Hinweis: Wenn PXE-Repräsentanten in Subnetzen des Netzwerks ausgeführt werden und Änderungen der Eingabeaufforderung für den PXE-Start auf einem dieser Proxies implementiert werden sollen, müssen Sie das Skript "PXE-Repräsentantenverteilung" auf dem Proxy ausführen.

So konfigurieren Sie Optionen der Eingabeaufforderung für den PXE-Start

1. Klicken Sie auf **Konfigurieren** | **Management Suite-Dienste** und anschließend auf das Register **Betriebssystem-Verteilung**.
2. Geben Sie einen Wert (in Sekunden) in das Feld "Timeout" ein. Standardmäßig werden 4 Sekunden verwendet. Es können maximal 60 Sekunden eingegeben werden.
3. Geben Sie eine Meldung in das Textfeld "Meldung" ein. Standardmäßig wird die Meldung "Drücken Sie F8, um das Menü anzuzeigen" angezeigt. Es können maximal 75 Zeichen eingegeben werden.
4. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, oder auf **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen.

So implementieren Sie Änderungen der Eingabeaufforderung für den PXE-Start auf einem PXE-Repräsentanten

1. Klicken Sie auf **Extras** | **Geplante Tasks** und anschließend in der Symbolleiste auf die Schaltfläche **Skript planen**.
2. Wählen Sie das Skript **PXE-Repräsentantenverteilung** in der Liste aus, und klicken Sie auf **OK**.
3. Verschieben Sie den PXE-Repräsentanten mittels Ziehen und Ablegen von der Netzwerkansicht in die Rechnerliste.
4. Wählen Sie das Skript **PXE-Repräsentantenverteilung** aus.

5. Klicken Sie in der Symbolleiste auf die Schaltfläche **Startzeit festlegen** (oder klicken Sie mit der rechten Maustaste auf den Task, und wählen Sie **Startzeit festlegen**), um das Skript sofort oder zu einem späteren Zeitpunkt auszuführen. Dieses Skript aktualisiert die Einstellungen der PXE-Startoption auf dem gewünschten PXE-Repräsentanten.

Verwenden von "Von LANDesk gesteuertes Starten"

"Von LANDesk gesteuertes Starten" ist die Standardoption für das Starten, wenn ein PXE-fähiger Client startet und für sich ein fehlgeschlagenes Abbildbereitstellungs- oder DOS-Task-Skript in der Core-Datenbank ermittelt. Sie können diese Startoption auch manuell auf dem Client auswählen, wenn das Startoptionsmenü angezeigt wird.

Da mit "Von LANDesk gesteuertes Starten" unbeaufsichtigte Bereitstellungen möglich sind, eignet sich diese Option, um bereits vorab Ziel-Clients für die Abbildverarbeitung anzugeben. So können Sie beispielsweise vor dem Einfügen neuer Clients in ein Netzwerk ein bestimmtes Betriebssystemabbild für diese Clients angeben, indem Sie eine .CSV-Datei mit den MAC-Adressen der Clients in die Core-Datenbank importieren. Weitere Informationen finden Sie unter "Verwenden von CSVIMPORT.EXE zum Importieren von Inventardaten" in Anhang B.

So geben Sie vorab Ziel-Clients mit der Option "Von LANDesk gesteuertes Starten" an

1. Bevor die PXE-fähigen Clients in das Netzwerk integriert werden, fügen Sie ihre Identifikationen durch Importieren einer .CSV-Datei in die Core-Datenbank ein.
2. Planen Sie einen Abbildbereitstellungsauftrag für die Clients.
3. Der Abbildverarbeitungsauftrag schlägt fehl, weil die Clients noch nicht mit dem Netzwerk verbunden sind.
4. Fügen Sie die Clients in das Netzwerk ein, und starten Sie sie.
5. Die Clients erkennen einen fehlgeschlagenen Abbildverarbeitungsauftrag und verwenden standardmäßig die Option "Von LANDesk gesteuertes Starten".
6. Der zuvor fehlgeschlagene Abbildbereitstellungsauftrag wird automatisch ausgeführt, und für die Ziel-Clients wird ein Abbild erstellt.

Verwenden des PXE-Startmenüs

Mit dem PXE-Startmenü können Sie ein Abbildbereitstellungsskript interaktiv für einen Client auswählen, ohne einen Abbildbereitstellungsauftrag planen zu müssen. Diese Methode kann hilfreich sein, wenn für beschädigte Clients neue Abbilder erstellt werden müssen. Bevor Sie das PXE-Startmenü verwenden, müssen Sie es zunächst konfigurieren, indem Sie die Betriebssystem-Verteilungsskripts hinzufügen, die im Menü angezeigt werden sollen.

Sie erstellen das PXE-Startmenüsystem, indem Sie Verzeichnisse erstellen und vorkonfigurierte Betriebssystem-Verteilungsskripts in diesen Verzeichnissen ablegen. Die Skriptbeschreibung wird als Menüelement im PXE-Startmenü des Clients angezeigt.

So konfigurieren Sie das PXE-Startmenü

1. Klicken Sie auf **Extras** | **PXE-Startmenü**.

2. Um ein neues Verzeichnis oder Unterverzeichnis im Menüsystem einzufügen, klicken Sie in der Symbolleiste auf die Schaltfläche **Neu** (oder klicken Sie mit der rechten Maustaste auf das übergeordnete Verzeichnis, und wählen Sie **Neu**).

   Hinweis: Das übergeordnete Verzeichnis kann vier Unterverzeichnisebenen besitzen.

3. Geben Sie einen Namen für das Verzeichnis ein. Im Verzeichnisnamen kann beispielsweise die Betriebssystemplattform oder Versionsnummer der im Verzeichnis enthaltenen Abbilder wiedergegeben werden. Sie können den Verzeichnisnamen jederzeit ändern, indem Sie in der Symbolleiste auf die Schaltfläche **Umbenennen** klicken (oder mit der rechten Maustaste auf das Verzeichnis klicken und **Umbenennen** auswählen).
4. Klicken Sie auf **Extras | Skripte verwalten**, und fügen Sie die Abbildungsbereitstellungsskripts mittels Ziehen und Ablegen in das entsprechende Verzeichnis im Fenster "PXE-Startmenü" ein.

   Hinweis: In jedem Verzeichnis können maximal 18 Skripts abgelegt werden.

5. Um das PXE-Startmenü zu speichern, klicken Sie in der Symbolleiste auf die Schaltfläche **Aktualisierung**. (Beachten Sie, dass Sie in der Konsole auf die Schaltfläche "Aktualisierung" klicken müssen, wenn die Änderungen beim Starten im PXE-Startmenü auf PXE-Clients angezeigt werden sollen.)

So greifen Sie vom Client auf das PXE-Startmenü zu

1. Starten Sie einen PXE-fähigen Client.
2. Wenn die Eingabeaufforderung für den PXE-Start angezeigt wird, drücken Sie vor Ablauf des Zeitintervalls die Funktionstaste **F8**. Wählen Sie **PXE-DOS-Menü**. Das Menüsystem, das Sie im Fenster "PXE-Startmenü" der Konsole konfiguriert haben, wird angezeigt.
3. Um ein Verzeichnis zu öffnen und seine Unterverzeichnisse und Abbilder anzuzeigen, geben Sie die Verzeichnisnummer ein, und drücken Sie die **Eingabetaste**. Navigieren Sie im Menüsystem, und suchen Sie nach dem Abbild, das auf dem Client bereitgestellt werden soll. Sie können **B** drücken, um eine Ebene zurückzugehen, oder **X**, um das Menüsystem zu beenden.

   Hinweis: Wenn Sie das Menüsystem beenden, ohne eine Auswahl zu treffen, wartet der Client auf einen geplanten Abbildverarbeitungsauftrag aus Management Suite.

4. Um ein Betriebssystemabbild (auf das in einem Betriebssystem-Verteilungsskript verwiesen wird) auszuwählen, geben Sie die Nummer des Skripts ein, und drücken Sie die **Eingabetaste**. Das Skript wird ausgeführt, und das Abbild wird auf den Client geladen.

Verwenden der PXE-Haltewarteschlange

Die PXE-Haltewarteschlange ist eine weitere Methode zur Fernbereitstellung von Betriebssystemabbildern auf PXE-fähigen Clients. In folgenden Situationen ist diese Methode besonders hilfreich:

- In einer gesteuerten Testumgebung, wenn die Abbilder aller Clients häufig durch identische Abbilder ersetzt werden.
- Für die Abbildverarbeitung von "Bare-Metal"-Clients in einer Testumgebung, die anschließend in ihre Produktionsumgebung übernommen werden können.

Wenn Sie den PXE-Repräsentanten eines Subnetzes als PXE-Haltewarteschlange angeben, werden alle PXE-fähigen Clients in diesem Subnetz automatisch in die PXE-Haltewarteschlange in der Netzwerkansicht der Konsole eingefügt, sobald der PXE-Start erfolgt. Sie können einen Client auch zu einer PXE-Haltewarteschlange hinzufügen, indem Sie das Skript "Zu PXE-Warteschlange hinzufügen" auf dem Client planen, oder indem Sie den Client in der Netzwerkansicht direkt in die PXE-Haltewarteschlangengruppe kopieren. Anschließend kann für die Clients ein Abbildbereitstellungsauftrag geplant werden.

So konfigurieren Sie eine PXE-Haltewarteschlange

1. Richten Sie PXE-Repräsentanten im Netzwerk ein.
2. Klicken Sie auf **Konfigurieren | Management Suite-Dienste** und anschließend auf das Register **Betriebssystem-Verteilung**.
3. Wählen Sie die PXE-Repräsentanten aus, und verschieben Sie sie von der Liste "Verfügbare Proxies" in die Liste "Haltewarteschlangen-Proxies.

   Die Liste "Verfügbare Proxies" enthält alle im Netzwerk vorhandenen PXE-Repräsentanten; sie werden mit ihrem Clientnamen angegeben. Diese Liste wird mit Hilfe des Inventarscanners generiert, mit dem die auf dem Client ausgeführte PXE-Software (PXE- und MTFTP-Protokolle) ermittelt wird. Der Inventarscanner wird automatisch ausgeführt, wenn ein PXE-Repräsentant erstmals eingerichtet wird.

4. Klicken Sie auf **Zurücksetzen**. Damit bewirken Sie, dass alle PXE-fähigen Clients, die sich im selben Subnetz wie der ausgewählte PXE-Repräsentant befinden, wieder in die PXE-Haltewarteschlange in der Netzwerkansicht der Konsole eingefügt werden. Für diese Clients kann dann ein Abbildverarbeitungsauftrag geplant werden.

   Hinweis: Die Schaltfläche "Zurücksetzen" wird aktiviert, wenn Sie einen PXE-Repräsentanten in der Liste "Haltewarteschlangen-Proxies" auswählen.

5. Klicken Sie auf **Übernehmen** und auf **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen.

Wenn das nächste Mal ein Client in diesem Subnetz gestartet wird, wird er in das Objekt "PXE-Haltewarteschlange" in der Netzwerkansicht der Konsole eingefügt.

So stellen Sie ein Abbild für einen Client in der PXE-Haltewarteschlange bereit

1. Klicken Sie auf **Extras | Geplante Tasks** und anschließend in der Symbolleiste auf die Schaltfläche **Skript planen**.
2. Wählen Sie ein Betriebssystem-Verteilungsskript in der Liste aus, und klicken Sie auf **OK**.
3. Öffnen Sie in der Netzwerkansicht der Konsole das Objekt **PXE-Haltewarteschlange**, und wählen Sie die Ziel-Clients aus, für die das Abbild bereitgestellt werden soll.
4. Fügen Sie die ausgewählten Clients mittels Ziehen und Ablegen in das Fenster "Geplante Tasks" ein.
5. Klicken Sie in der Symbolleiste auf die Schaltfläche **Startzeit festlegen**, um das Skript sofort oder zu einem späteren Zeitpunkt auszuführen.

Übersicht über die Profilmigration

Die Profilmigration und die Betriebssystem-Verteilung bilden zusammen eine komplette Bereitstellungs- und Migrationslösung. Mit der Profilmigration ist es möglich, beim Aktualisieren oder Migrieren alle angepassten Desktop- und Anwendungseinstellungen der Benutzer sowie persönlichen Datendateien beizubehalten. Die Profilmigration unterstützt Direktmigrationen einzelner Clients sowie umfangreiche Fernmigrationen mehrerer Clients über das Netzwerk.

Die Profilmigration ist als zweigeteilter Prozess zu verstehen:

1. *Erfassen* des eindeutigen Profils eines Quell-Clients, bestehend aus Benutzerkonten, Desktop(PC)- und Anwendungseinstellungen sowie Datendateien.
2. *Wiederherstellen* des Profils auf einem Ziel-Client.

Schrittanweisungen für die Profilerfassung und das Wiederherstellungsverfahren finden Sie unter "Erstellen von Migrationsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten" weiter oben in diesem Kapitel.

Ausführliche Beschreibungen der einzelnen Seiten der Assistentenoberfläche finden Sie im Abschnitt "Hilfe zum Betriebssystem-Verteilung/Migrationstasks-Assistenten" in Anhang B.

Migrationsmethoden: mit Skript und benutzerinitiiert

Bei Verwendung der Profilmigration können Sie mit Hilfe des Betriebssystem-Verteilung/Migrationstasks-Assistenten separate Erfassungs- und Wiederherstellungsskripts erstellen. Die Skripts können anschließend entfernt auf einem oder mehreren Ziel-Clients im Netzwerk ausgeführt werden.

Darüber hinaus können Sie in der Konsole selbstextrahierende ausführbare Dateien (benutzerinitiierte Pakete genannt) erstellen, die Sie oder der Endbenutzer direkt von den einzelnen Clients als benutzerinitiierte Profilmigration ausführen können. Das benutzerinitiierte Paket startet den LANDesk-Profilmigrationsassistenten. Weitere Informationen finden Sie unter "Erstellen von benutzerinitiierten Profilmigrationspaketen" weiter unten in diesem Kapitel.

Beide Migrationsmethoden verfolgen denselben Zweck, es gibt allerdings einige unterschiedliche Funktionen. Mit der direkten benutzerinitiierten Methode können Sie beispielsweise auswählen, welche Benutzerkonten migriert werden sollen, während dies bei der Methode mit dem geplanten Skript nicht möglich ist. Die folgenden Informationen betreffen insbesondere die Skriptmethode. Der Betriebssystem-Verteilung/Migrationstasks-Assistent enthält eine eigene Online-Hilfe, in der die Funktionen dieses Dienstprogramms beschrieben werden. Bei Verwendung des Assistenten können Sie auf jeder Assistentenseite auf "Hilfe" klicken, um weitere Informationen abzurufen.

Migrationspfade

Die Profilmigration unterstützt die Migration zwischen folgenden Versionen von Windows-Betriebssystemen:

- Von Windows 95 und 98 SE...nach Windows 2000 SP3 oder Windows XP
- Von Windows NT 4 ...nach Windows 2000 SP3 oder Windows XP
- Von Windows 2000 ...nach Windows 2000 SP3 oder Windows XP
- Von Windows XP ...nach Windows XP
- Windows Server 2003 wird ebenfalls unterstützt (sowohl für Erfassung als auch für Wiederherstellung)

Voraussetzungen

Eine Profilmigration ist nur möglich, wenn Clients folgende Voraussetzungen erfüllen:

- Die Clients müssen in der Core-Datenbank enthalten sein.
- Auf den Clients müssen die CBA-, Enhanced Software Distribution- und Inventaragenten geladen sein. Die Profilmigration verwendet den Enhanced Software Distribution-Agenten zum Verteilen von Dateien.

Profilinhalt

Mit der Profilmigration können Sie folgende Inhalte migrieren:

- Benutzerkonten
- Anwendungseinstellungen, Vorlagen und verknüpfte Dateien
- Desktop(PC)-Einstellungen
- Dateien und Ordner

Benutzerkonten werden standardmäßig migriert. Einstellungen und Dateien werden entsprechend einer benutzerdefinierten Regelsammlung migriert (weitere Informationen finden Sie im Anschluss unter "Erstellen von Sammlungen"). Sie können Regeln für Anwendungen, Desktop-Einstellungen sowie Dateien und Ordner erstellen.

Erstellen von Sammlungen

Verwenden Sie das Dialogfeld "Regelsammlung", um neue Sammlungen zu erstellen und vorhandene Sammlungen zu bearbeiten. Eine Sammlung ist eine benutzerdefinierte Gruppe von Anwendungs-, Desktop- und Dateiregeln, die den Profilinhalt festlegen, der vom Migrationsskript migriert (erfasst oder wiederhergestellt) werden soll.

So erstellen Sie eine Sammlung

1. Um das Dialogfeld "Regelsammlung" zu öffnen, klicken Sie zuerst in der Symbolleiste des Fensters "Skripte verwalten" auf die Schaltfläche **Sammlungsmanager**. Wählen Sie anschließend **Sammlungen**, und klicken Sie auf **Neu**. Sie können dazu auch den Betriebssystem-Verteilung/Migrationstasks-Assistenten verwenden, indem Sie auf der Assistentenseite "Sammlung für dieses Profil auswählen" auf die Schaltfläche **Verwalten** klicken.
2. Geben Sie einen eindeutigen Namen für die Sammlung ein.
3. (Optional) Geben Sie eine Beschreibung ein, die den mit dieser Sammlung erfassten/wiederhergestellten Profilinhalt wiedergibt.
4. Definieren Sie den Inhalt, der mit der Sammlung erfasst/wiederhergestellt werden soll, indem Sie Regeln in der Liste "Regeln" auswählen. Mit den Plus- und Minuszeichen können Sie die Baumstruktur ein- bzw. ausblenden und alle Anwendungen, Desktop-Einstellungen und Dateiregeln anzeigen.

   Um eine Regel auszuwählen, aktivieren Sie das entsprechende Kontrollkästchen; zur Definition einer Sammlung können Sie die in der Strukturansicht "Regeln" angezeigten Regeln beliebig kombinieren.

5. Klicken Sie auf "OK", um die Sammlung zu speichern und zum Dialogfeld "Sammlungsmanager" zurückzukehren.

Hinweis: Wenn Sie eine Sammlung löschen, wird diese Sammlung vom Core Server entfernt. Migrationsskripts, die auf diese Sammlung Bezug nehmen, werden nicht ordnungsgemäß ausgeführt. Sie sollten auch das betreffende Skript löschen.

Migrieren von Benutzerkonten

Bei einer Skriptprofilmigration werden standardmäßig alle entdeckten lokalen und Domänenbenutzerkonten auf den Quell-Clients erfasst (**Wichtig:** außer die Konten "Alle Benutzer" und "Standardbenutzer").

Alle erfassten Benutzerkonten werden auf den Ziel-Clients wiederhergestellt. Ein Benutzerkonto, das noch nicht auf dem Ziel-Client vorhanden ist, wird als neues lokales Benutzerkonto erstellt, und seine Einstellungen werden migriert. Vor dem Wiederherstellen von Benutzerkonten können Sie ein Standardkennwort für diese neuen lokalen Benutzerkonten eingeben. Wenn auf dem Ziel-Client bereits ein doppeltes Benutzerkonto vorhanden ist, werden die erfassten Einstellungen des (Quell-)Benutzerkontos auf das vorhandene Benutzerkonto migriert, das aktuelle Kennwort des Benutzers wird jedoch beibehalten und sollte zum Anmelden verwendet werden.

Migrieren von Anwendungseinstellungen, Vorlagen und verknüpften Dateien

Die ständigen Einstellungen, Vorlagen- und verknüpften Dateien einer Anwendung können als Teil eines Clientprofils migriert werden. Die Anwendungsprogramme selbst werden bei der Profilmigration *nicht* migriert (sie können jedoch zusammen mit dem Betriebssystemabbild bereitgestellt werden). Jede Anwendungsmigration wird durch eine Anwendungsregel definiert, die einer Regelsammlung hinzugefügt werden kann.

Anwendungsregeln stehen für folgende Anwendungen zur Verfügung:

- **Microsoft Access**
  - *Unterstützte Versionen:* 95, 97, 2000 und XP
  - *Migrierte Dateien:* *.ade; *.adp;* .mad; *.maf; *.mag; *.mam; *.maq; *.mar; *.mas; *.mat; *.mav; *.maw; *.mda; *.mdb; *.mdbhtml; *.mde; *.mdt; *.mdz; *.mdw

- **Microsoft Excel**
  - *Unterstützte Versionen:* 95, 97, 2000 und XP
  - *Migrierte Dateien:* *.xls; *.csv; *.dqy; *.iqy; *.oqy; *.rqy; *.slk; *.xla; *.xlb; *.xlc; *.xld; *.xlk; *.xll; *.xlm; *.xls; *.xlshtml; *.xlv; *.xlw; *.dif; *.xlt; *.xlthtml

- **Microsoft Outlook**
  - *Unterstützte Versionen:* 95, 97, 2000 und XP
  - *Migrierte Dateien:* *.ics; *.msg; *.oft; *.pst; *.vcs; *.pab; *.rwz; *.oab; *.oft; *.srs

- **Microsoft PowerPoint**
  - *Unterstützte Versionen:* 95, 97, 2000 und XP
  - *Migrierte Dateien:* *.ppt; *.ppthtml; *.pps; *.ppa; *.pwz; *.ppz; *.pp1

- **Microsoft Word**
  - *Unterstützte Versionen:* 95, 97, 2000 und XP

  - *Migrierte Dateien:* *.doc; *.dochtml; *.gly; *.rtf; *.wbk; *.wiz

- **Gemeinsam genutzte Microsoft Office-Komponenten**
  - *Unterstützte Versionen:* 95, 97, 2000 und XP
  - *Migrierte Dateien:* Autokorrekturlisten (*.acl), Benutzerwörterbücher (*.dic), Standardsymbolleisten und alle Vorlagendateien für unterstützte Office-Anwendungen, einschließlich: *.dot; *.dothtml; *.htm; *.pot; *.pothtml; *.xlt; *.xlthtml; *.mdn; *.mdz; *.wizhtml

- **Microsoft Internet Explorer**
  - *Unterstützte Versionen:* 4.0, 5.0, 5.5 und 6.0
  - *Migrierte Dateien:* Favoriten (*.*), Cookies (*.txt, *.dat) und Bewertungsdateien (*.rat)

Unterstützung neuer Anwendungen bei Management Suite 8

Für folgende Anwendungen stehen nun Anwendungsregeln zur Verfügung:

- ACT!
- Adobe Acrobat
- Adobe Acrobat Reader
- Adobe Illustrator
- Adobe PageMaker
- Adobe Photoshop
- Lotus 1-2-3
- Lotus Approach
- Lotus FastSite
- Lotus Freelance
- Lotus Notes
- Lotus Organizer
- Lotus SmartCenter
- Lotus Word Pro
- MS ActiveSync
- MS FrontPage
- MS NetMeeting
- MS Outlook Express
- MS Visio
- Netscape
- Palm Desktop
- WinZip
- Yahoo Messenger

Anmerkungen zur Anwendungsmigration

- Migrationen von Aktualisierungsversionen werden für Office 95 und 97 auf Office 2000 oder XP unterstützt. Für Office 2000 und Office XP können Sie Anwendungen auf dieselbe Version migrieren.
- Wenn eine Anwendung nicht auf dem Ziel-Client installiert ist, werden die Einstellungen und Dateien dieser Anwendung *nicht* migriert, selbst wenn sie auf dem Quell-Client erfasst wurden.

- Beachten Sie, dass Vorlagendateien für alle angegebenen Microsoft-Anwendungen als Teil der Regel für gemeinsam genutzte Microsoft-Komponenten migriert werden. Um Vorlagendateien zu migrieren, müssen Sie "Freigegebene Komponenten" auswählen.
- Um eine erfolgreiche Migration aller zuletzt gültigen Einstellungen und Dateien zu gewährleisten, müssen Sie alle Anwendungen schließen, bevor Sie eine Profilmigration ausführen.

Weitere Anwendungsunterstützung

Die neuesten Anwendungsregeldateien von LANDesk Software finden Sie auf der LANDesk-Supportsite unter http://www.landesk.com/support/downloads/index.php.

Migrieren von Desktop(PC)-Einstellungen

Viele der angepassten und optimierten Einstellungen auf Clients können ebenfalls migriert werden. Jede Migration von Einstellungen wird durch eine Desktop-Regel definiert, die einer Regelsammlung hinzugefügt werden kann.

Sie können folgende Desktop(PC)-Einstellungen migrieren:

- Desktop-Verknüpfungen, Dateien, Ordner und Aktenkoffer

  Hinweis zu Aktenkoffern: Vor der Migration eines Aktenkoffers müssen Sie "Alles aktualisieren" dafür ausführen. Wenn der Aktenkoffer Verknüpfungen auf Dateien in einem "benutzerspezifischen" Verzeichnis enthält, das sich je nach Betriebssystem ändert, und Sie auf ein anderes Betriebssystem migrieren, werden zwar die Dateien migriert, die Verknüpfungen gehen jedoch verloren und müssen neu erstellt werden.

- Ordner "Eigene Dateien"
- Verbundene Netzlaufwerke

  Hinweis zu doppelten Laufwerksbuchstaben Wenn auf dem Ziel-Client bereits ein Laufwerksbuchstabe zugeordnet ist, wird dieses zugewiesene Laufwerk nicht ersetzt, sondern behalten. Die Laufwerksbuchstabenzuordnung des Quell-Clients wird nicht migriert.

- Drucker (Netzwerk)
- Hintergrund
- Bildschirmauflösung, Farbqualität und Aktualisierungsrate

Migrieren von Dateien und Ordnern

Mit eigenen, angepassten Dateiregeln können Sie einzelne oder mehrere Dateien migrieren, indem Sie das Verzeichnis und den Dateinamen angeben. Dateiregeln bieten hilfreiche Steuerungsfunktionen und Flexibilität, weil Sie damit folgende Möglichkeiten haben:

- Erstellen beliebig vieler Dateiregeln, die Sammlungen hinzugefügt werden

- Ein- und/oder Ausschließen von Dateien durch Platzhalternamen in einer Einzeldateiregel
- Angeben, ob Unterverzeichnisse berücksichtigt werden sollen
- Umleiten von Dateien in ein neues Verzeichnis auf dem Ziel-Client
- Erfassen von Dateien von einer Festplatte auf dem Quell-Client (einschließlich Festplattenpartitionen) und erfolgreiches Migrieren der Dateien, selbst wenn der Ziel-Client nicht dieselbe Partitionierung aufweist
- Beibehalten der Verzeichnisstruktur der erfassten Datei; wenn die Verzeichnisstruktur einer erfassten Datei auf dem Ziel-Client nicht vorhanden ist, wird der Pfad erstellt und die Datei darin wiederhergestellt

Sie können Dateien von den *Festplatten*, einschließlich Festplattenpartitionen, eines Clients migrieren. Wechselmedien, wie z. B. CD-ROM-Laufwerke, und Netzwerkfreigaben werden nicht unterstützt. Falls der Ziel-Client nicht über einen entsprechenden Laufwerksbuchstaben für die Festplattenpartition verfügt, wird im Stammverzeichnis des Laufwerks C des Clients ein neues Verzeichnis namens "Migrated_[Laufwerksbuchstabe]_Drive" angelegt, und die Dateien werden (zusammen mit der zugehörigen Verzeichnisstruktur) in dieses neue Verzeichnis migriert.

So erstellen Sie eine Dateiregel

Verwenden Sie das Dialogfeld "Dateiregeln", um neue Dateiregeln zu erstellen oder vorhandene Dateiregeln zu bearbeiten. Eine Dateiregel legt anhand folgender Kriterien fest, welche Dateien migriert werden: Laufwerk- und Verzeichnisspeicherort, Unterverzeichnisse, Dateibenennung einschließlich Platzhalterunterstützung und Zielspeicherort.

1. Klicken Sie im Dialogfeld "Sammlungsmanager" auf **Dateiregeln** und anschließend auf **Neu**, um das Dialogfeld "Dateiregeln" zu öffnen.
2. Geben Sie einen eindeutigen Namen für die Dateiregel ein.
3. (Optional) Geben Sie eine Beschreibung ein, die den Inhalt der Dateiregel wiedergibt.
4. Geben Sie alle Optionen im Dialogfeld ein (Beschreibungen der Optionen finden Sie unter "Informationen zum Dialogfeld "Dateiregel"".)
5. Klicken Sie auf **OK**, um die Dateiregel zu speichern und zum Dialogfeld "Sammlungsmanager" zurückzukehren.

Wenn Sie eine Dateiregel löschen, wird sie vom Core Server entfernt. Jede Sammlung, die diese Regel enthielt, weist auf diese Änderung hin, wenn Sie die Sammlung das nächste Mal öffnen oder bearbeiten.

Weitere Anmerkungen zur Dateimigration

- **Regeln und Sammlungen:** Sie können beliebig viele Dateiregeln erstellen. Anschließend fügen Sie die Dateiregeln Sammlungen hinzu, die u. U. bereits andere Regeln für Dateien, Anwendungs- und Desktop-Einstellungen enthalten.
- **Dateipfad (Verzeichnisstruktur):** Die einer Datei zugewiesene Verzeichnisstruktur wird standardmäßig beibehalten.

- **Mehrere Steuerungen in einer Dateiregel:** Eine Dateiregel kann beliebige Kombinationen mehrerer Steuerungen für den Ein- oder Ausschluss von Dateien enthalten.
- **Umgang mit Dateiersetzungen:** Die Datei auf dem Ziel-Client wird durch die auf dem Quell-Client erfasste Datei ersetzt, SOFERN die erfasste Datei neuer als der Änderungsdatum-Zeitstempel für die vorhandene Datei ist.
- **Beschränkung der Dateigröße:** Da Profildaten in aufeinander folgenden .CAB-Windows-Dateien mit einer Größenbeschränkung von 2 GB gespeichert werden, können Einzeldateien, die größer als 2 GB sind, nicht migriert werden. Auf Clients gibt es zwar nur selten Dateien dieser Größe, dennoch sollten Sie wissen, dass es diese Beschränkung gibt.

Erstellen von Migrationsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten

Die folgende Schrittanweisung beschreibt das Erfassen und Wiederherstellen eines Clientprofils mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten. Um weitere Informationen zu den einzelnen Schritten zu erhalten, klicken Sie auf die Schaltfläche **Hilfe**, die auf jeder Seite des Skriptassistenten angezeigt wird.

Hinweis: Informationen zur Erfassung und Wiederherstellung eines Profils mit einem benutzerinitiierten Migrationspaket finden Sie in der Online-Hilfe des LANDesk-Profilmigrationsassistenten.

So erstellen Sie ein Profilerfassungsskript

1. Klicken Sie auf **Extras | Skripte verwalten**.
2. Klicken Sie im Fenster "Skripte verwalten" mit der rechten Maustaste auf **Alle OSD-/Profilmigrationsskripts**, anschließend klicken Sie im Kontextmenü auf **Neues OSD-/Profilmigrationsskript**, um den Assistenten zu öffnen. Oder klicken Sie im Fenster "Skripte verwalten" in der Symbolleiste auf die Schaltfläche **Neues OSD-/Profilmigrationsskript**.
3. Wählen Sie **Profil aufnehmen**, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie einen Namen und eine Beschreibung für das Profilerfassungsskript ein, und klicken Sie auf **Weiter**.
5. Wählen Sie eine vordefinierte Regelsammlung aus (die den Profilinhalt festlegt), und klicken Sie auf **Weiter**.
6. Geben Sie einen UNC-Pfad und -Berechtigungsnachweise für die Authentifizierung für das Verzeichnis ein, in dem die Profildaten gespeichert werden sollen.
7. Klicken Sie auf **Fertigstellen**, um das Profilerfassungsskript zu erstellen und den Assistenten zu beenden.

Mit "Geplante Tasks" können Sie nun die Ausführung des Skripts auf einem oder mehreren Ziel-Clients im Netzwerk planen.

Speichern von Profildaten für mehrere Clients (und mehrere Benutzer)

Profildaten werden in .CAB-Windows-Dateien in einer Verzeichnisstruktur gespeichert, die sich unter dem angegebenen UNC-Pfad befindet. Wenn Sie ein Profilerfassungsskript auf mehreren Clients ausführen, werden die Profildaten der einzelnen Clients in separaten Verzeichnissen gespeichert, die entsprechend ihren eindeutigen Windows-Computernamen benannt werden. Genauso verhält es sich auch mit Benutzern: Wenn mehrere Benutzer auf demselben Quell-Client ermittelt und erfasst werden, werden die Profildaten der einzelnen Benutzer in separaten Unterverzeichnissen (des Clientverzeichnisses) gespeichert, die entsprechend dem Benutzeranmeldenamen benannt werden. Anders ausgedrückt: Jeder migrierte Client besitzt ein eigenes Profilspeicherverzeichnis und ein Unterverzeichnis für jedes erfasste Benutzerkonto auf diesem Client.

So erstellen Sie ein Profilwiederherstellungsskript

1. Klicken Sie auf **Extras | Skripte verwalten**.
2. Klicken Sie im Fenster "Skripte verwalten" mit der rechten Maustaste auf **Alle OSD-/Profilmigrationsskripts**, anschließend klicken Sie im Kontextmenü auf **Neues OSD-/Profilmigrationsskript**, um den Assistenten zu öffnen. Oder klicken Sie im Fenster "Skripte verwalten" in der Symbolleiste auf die Schaltfläche **Neues OSD-/Profilmigrationsskript**.
3. Wählen Sie **Profil wiederherstellen**, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie einen Namen und eine Beschreibung für das Profilwiederherstellungsskript ein, und klicken Sie auf **Weiter**.
5. Geben Sie den UNC-Pfad und -Berechtigungsnachweise für die Authentifizierung für das Verzeichnis der Profildaten ein, die wiederhergestellt werden sollen, und geben Sie ein Standardkennwort für migrierte, neue lokale Benutzerkonten ein (wird kein Wert eingegeben, so wird automatisch "Kennwort" vorgegeben).
6. Klicken Sie auf **Fertigstellen**, um das Profilwiederherstellungsskript zu erstellen und den Assistenten zu beenden.

Mit "Geplante Tasks" können Sie nun die Ausführung des Skripts auf einem oder mehreren Ziel-Clients im Netzwerk planen.

Hinweis: Windows 2000 SP3 und Windows XP sind die einzigen unterstützten Betriebssysteme für *Ziel-Clients*.

Protokolldatei der Profilmigration

Bei der Profilmigration (sowohl bei der Skript- als auch bei der benutzerinitiierten Methode) wird eine Protokolldatei mit dem Namen PROFILEMIGRATION.LOG erstellt, die laufend aktualisiert und im benutzerspezifischen Verzeichnis für Profildaten gespeichert wird. Relevante Informationen, wie Zeit, jeweilige Operation und Status, werden der vorhandenen Protokolldatei für jede weitere Erfassung und Wiederherstellung angehängt. Wenn die Protokolldatei eine Größe von 64 KB erreicht, wird sie in PROFILEMIGRATION.OLD umbenannt, und es wird eine neue .LOG-Datei erstellt. Sie können diese Protokolldatei in einem beliebigen Texteditor anzeigen.

Erstellen von benutzerinitiierten Profilmigrationspaketen

Im Dialogfeld "Benutzerinitiiertes Paket" können Sie eine selbstextrahierende ausführbare Datei erstellen, die als benutzerinitiierte Profilmigration auf Clients ausgeführt werden kann.

Benutzerinitiierte Migrationspakete können sowohl auf Clients als auch auf Computern, die nicht mit Management Suite ausgestattet sind, ausgeführt werden.

So erstellen Sie ein benutzerinitiiertes Migrationspaket

1. Öffnen Sie das Dialogfeld "Sammlungsmanager" im Betriebssystem-Verteilung/Migrationstasks-Assistenten oder indem Sie auf **Skripte | Sammlungsmanager** klicken.
2. Wählen Sie **Benutzerinitiiertes Paket**, und klicken Sie anschließend auf **Neu**.
3. Geben Sie einen eindeutigen Namen für das Paket ein. Geben Sie hier keine Dateinamenerweiterung ein. Die Erweiterung .EXE wird automatisch angehängt.
4. Wählen Sie eine Sammlung in der angezeigten Liste aus. Die ausgewählte Sammlung bestimmt die Anwendungen, Desktop-Einstellungen und Dateien des Profilinhalts. Sie können nur eine Sammlung pro Migrationspaket auswählen.
5. Um das Paket zu erstellen, klicken Sie auf **OK**. Dieser Vorgang kann einige Zeit in Anspruch nehmen, je nachdem, wie groß der Profilinhalt ist, der in der ausgewählten Sammlung definiert wurde.

Das benutzerinitiierte Migrationspaket (.EXE) wird standardmäßig im folgenden Verzeichnis auf dem Core Server gespeichert: c:\Program Files\LANDesk\ManagementSuite\LDLogon\PMScripts\Executables.

Wenn Sie ein benutzerinitiiertes Paket löschen, wird es vom Core Server entfernt. Abhängig davon, wie und wo Sie das Paket an Benutzer verteilt haben, können möglicherweise noch andere Kopien des Pakets vorhanden sein.

Ausführen von benutzerinitiierten Profilmigrationspaketen

Sie können das benutzerinitiierte Migrationspaket per E-Mail oder über Wechselmedien an Clients verteilen und auf dem Client ausführen. Oder Sie speichern das Paket auf einer Netzwerkfreigabe und führen es von einem Client aus, der Zugriff auf diese Freigabe hat.

Das Paket startet den LANDesk-Profilmigrationsassistenten, der eine eigene Online-Hilfedatei besitzt. Um weitere Informationen zu erhalten, einschließlich Schrittanweisungen für die Erfassung und Wiederherstellung eines Profils mit benutzerinitiierten Migrationspaketen, klicken Sie auf einer beliebigen Seite des LANDesk-Profilmigrationsassistenten auf **Hilfe**.

Kapitel 10: Reparieren von beschädigten Anwendungen

Die Funktion "Application Healing" sorgt dafür, dass Anwendungen auf Clients funktionsfähig bleiben. Application Healing repariert automatisch Anwendungen, die wegen versehentlich gelöschten oder beschädigten Dateien nicht mehr funktionieren. Mithilfe von Application Healing können Sie LANDesk Management Suite so konfigurieren, dass die von Ihnen angegebenen Anwendungen repariert werden.

Wenn eine Anwendung auf einem Client nicht gestartet wird, sucht Application Healing nach dem Problem. Der Application Healing-Agent verwendet dann ein Enhanced Software Distribution (ESWD)-Paket, um die Komponenten dieser Anwendung neu zu installieren und korrigiert dabei etwaige Fehler. Um den Einsatz von Netzwerkbandbreite zu minimieren, werden bei der Reparatur nur fehlende, beschädigte oder veraltete Dateien auf den Client kopiert.

Mit Application Healing können Sie Anwendungen reparieren, die mit oder ohne ESWD-Paketen bereitgestellt wurden. Anwendungen, die ohne ESWD-Paket installiert wurden, können reparabel gemacht werden, indem ein ESWD-Paket für die Reparatur erstellt wird. Voraussetzung für Application Healing ist, dass Sie ESWD-Pakete für die Reparatur verwenden.

Sie können Application Healing auch für eine Überwachungsfunktion verwenden. Wenn Sie Application Healing-Agenten auf Clients bereitstellen, ohne Agenten für die Reparatur von bestimmten Anwendungen zu konfigurieren, berichten die Agenten dem Core Server, wenn eine Anwendung Probleme beim Starten hat. Sie können dann Berichte von der Konsole ausführen, um zu sehen, welche Anwendungen den Clients Probleme bereiten.

In diesem Kapitel erfahren Sie mehr über:

- Konfigurieren von Application Healing
- Konfigurieren von Schritt 1: Einrichten von ESWD-Paketen für die Reparatur
- Konfigurieren von Schritt 2: Herstellen der Reparaturfähigkeit für Anwendungen
- Konfigurieren von Schritt 3: Bereitstellen von ARL-Dateien auf Clients
- Anzeigen von Application Healing-Ereignissen
- Anzeigen von Application-Healing-Berichten
- Application Healing-Registrierungsschlüssel

Konfigurieren von Application Healing

Zur Installation von Application Healing müssen Sie die folgenden Schritte ausführen:

- Verwenden Sie den Client-Setup-Assistenten, um die Clients für Application Healing zu konfigurieren.

Für die Verwendung von Application Healing nach der Installation müssen Sie die folgenden Schritte ausführen:

- Richten Sie für jede Anwendung, die reparabel sein soll, ein ESWD-Paket ein.
- Konfigurieren Sie Anwendungsreparaturlisten (ARLs) für die Anwendungen, die reparabel sein sollen.
- Verteilen Sie die Anwendungsreparaturlisten auf die Clients.

Nachdem Sie Application Healing installiert haben:

- Wenn der Agent einen Anwendungsfehler erkennt, startet er den Reparaturvorgang mithilfe der ARL-Datei der Anwendung, die Sie zuvor gesendet haben. Aus der ARL entnimmt der Agent den ESWD-Paketpfad und verwendet das Paket, um zu bestimmen, welche Dateien neu installiert werden müssen.
- Der Agent sendet Ereignisse über den Software-Reparaturstatus an den Core Server. Prüfen Sie den Status in regelmäßigen Abständen mithilfe des AMS-Warnprotokolls und der Application Healing-Berichte.

Nachdem Sie die Unterstützung für Application Healing auf dem Core Server, den Verwaltungskonsolen und den Clients installiert haben, müssen Sie dafür sorgen, dass wichtige Anwendungen auf den Clients reparabel sind.

Sie müssen die folgenden Schritte durchführen:

- Richten Sie ESWD-Pakete für die Anwendungen ein, die reparabel sein sollen.
- Konfigurieren Sie Anwendungsreparaturlisten (ARLs) für die Anwendungen, die reparabel sein sollen.
- Verteilen Sie die Anwendungsreparaturlisten auf die Clients.

Wie Application Healing Anwendungsprobleme erkennt

Der Application Healing-Agent sucht nach Fehlern beim Starten von .EXEs (Prozesserstellung) oder Laden von .DLLs (Bibliothek laden). Der Agent protokolliert alle erkannten Fehler im AMS-Warnprotokoll auf dem Core Server des Clients. Wenn der Client nicht mit dem Netzwerk verbunden ist, speichert der Agent die Ereignisse lokal, bis er an den Core Server übermitteln kann.

Wenn ein Benutzer versucht, ein Programm über eine Verknüpfung zu starten und diese Verknüpfung nicht vorhanden ist, wird Application Healing nicht ausgelöst. Dies passiert, weil die betroffene Anwendung nie gestartet wurde und der Agent daher den Fehler nie erkennen konnte. Wenn jedoch ein Benutzer versucht, eine Anwendung durch Doppelklicken auf eine Datei zu starten, die mit der Anwendung verknüpft ist, wird Application Healing in der Regel ausgelöst, obwohl die ausführbare Hauptdatei der Anwendung, auf die die Verknüpfung verweist, fehlt.

Wenn eine .EXE- oder .DLL-Datei in einer ARL-Datei ein Problem verursacht, löst der Agent den Reparaturvorgang mithilfe von Informationen in der ARL-Datei aus. Wenn kürzlich ein Reparaturversuch stattgefunden hat (standardmäßig innerhalb der letzten 10 Minuten), versucht Application Healing nicht erneut, die Anwendung in diesem Intervall zu reparieren.

Wenn ein Reparaturversuch nicht in einem Intervall durchgeführt wurde, den Sie im Client-Setup-Assistenten angegeben haben, beginnt der Agent erneut mit der Installation der Anwendung mit dem ESWD-Paket, das in der ARL-Datei der Anwendung angegeben wurde.

Wenn es sich um einen Fehler beim Erstellungsprozess handelte, der den Reparaturvorgang ausgelöst hat und der Benutzer die sofortige Reparatur wählt, versucht Application Healing, die Anwendung neu zu starten, sobald die Reparatur abgeschlossen ist.

Konfigurieren von Schritt 1: Einrichten von ESWD-Paketen für die Reparatur

Voraussetzung für Application Healing ist ein ESWD-Installationspaket für die Anwendung, die Sie reparieren möchten. Wenn Sie ursprünglich das Anwendungspaket über ESWD verteilt haben und das Paket auf dem Netzwerk oder einem Webserver verfügbar ist, können Sie eine ARL erstellen.

Wenn Sie Anwendungen über eine andere Methode installiert haben, müssen Sie ein ESWD-Paket mit dem ESWD-Package Builder erstellen. Verwenden Sie beim Erstellen des Pakets dieselbe Konfiguration des ursprünglichen Pakets oder der Anwendungsinstallation. Wenn dagegen Application Healing das neue Paket für die Reparatur verwendet, können Installationsunterschiede (Speicherort der Dateien usw.) zu Problemen führen. Sie müssen außerdem das Ersatz-ESWD-Paket testen, bevor Sie es in einer Produktionsumgebung einsetzen.

Wenn Application Healing ein ESWD-Paket für die Reparatur einsetzt, wird während der Reparatur jede Benutzeroberfläche angezeigt, die Sie als Teil des Pakets angepasst haben. Wenn Sie möchten, dass sich die Reparaturpakete während der Installation anders als die Anwendungsinstallationspakete verhalten, benötigen Sie möglicherweise zwei Paketversionen.

Jedes ESWD-Paket hat eine eindeutige GUID. Application Healing verwendet diese GUID zum Abgleich der Paketversionen. Wenn z.B. die GUID eines Pakets mit der in der ARL-Datei gespeicherten GUID übereinstimmt, aktualisiert Application Healing nur fehlende oder geänderte Dateien. Wenn ESWD die Paketdateien lokal im Cache gespeichert hat, kann Application Healing mithilfe einer übereinstimmenden GUID die Dateien während der Reparatur aus dem Cache anstatt vom Netzwerk abrufen. Wenn eine Paket-GUID nicht mit dem Paket übereinstimmt, auf das ARL verweist, installiert Application Healing das gesamte Paket neu.

Konfigurieren von Schritt 2: Herstellen der Reparaturfähigkeit für Anwendungen

Nachdem Sie Clients für Application Healing konfiguriert haben und sich ein ESWD-Paket für die Anwendung, die Sie reparieren möchten, auf dem Netzwerk oder auf einem Webserver befindet, können Sie eine Anwendungsreparaturliste (ARL) erstellen. Eine ARL teilt dem Application Healing-Agenten mit, welche Anwendungen reparabel sind wo sie repariert werden sollen. Die ARL enthält die folgenden Informationen:

- Anwendungsname
- Zu überwachende auszuführende Datei oder .DLLs
- Pfad zum Paket, das die Anwendung repariert

Sie können mehrere Anwendungskonfigurationen zu einer ARL-Datei hinzufügen. Sie sollten die ARL-Dateien systematisch organisieren. Nachdem Sie sich entschieden haben, wie Sie die Dateien organisieren möchten, müssen Sie die ARLs erstellen und sie auf die Clients verteilen.

Erstellen von ARL-Dateien

Fenster "Application Healing"

Erstellen und verwalten Sie die ARL-Dateien über das Konsolenfenster "Application Healing". Das Fenster "Application Healing" enthält drei Spalten:

- **Anwendungsreparaturliste:** Die ARL-Dateien im Verzeichnis Programmdateien\Intel\DTM\ldlogon. Durch Auswahl einer ARL in dieser Spalte werden die anderen Spalten gefüllt und Sie können diese ARL konfigurieren.
- **Anwendungsname:** Der Name, den Sie für die Anwendung angegeben haben, die Sie konfigurieren.
- **Paketspeicherort:** Der URL- oder UNC-Pfad zum ESWD-Paket, das die Anwendung repariert, die Sie konfigurieren. Über diesen Pfad greifen Clients auf das Paket zu.
- **Dateiname:** Die Anwendungsdateien, die Application Healing auslösen, wenn es zu einem Problem kommt. Dabei sollte es sich um die wichtigsten .EXEs und .DLLs der Anwendung handeln, die am ehesten Fehler verursachen, wenn die Anwendung nicht richtig funktioniert.

So erstellen Sie eine Anwendungsreparaturliste

Wenn das Fenster "Application Healing" nicht angezeigt wird, klicken Sie auf **Extras | Application Healing**.

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue ARL** .
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Fügt die Anwendung zur ARL hinzu** .
3. Geben Sie den Namen der Anwendung ein, die Sie konfigurieren.

4. Geben Sie den Speicherort des Pakets ein, das die Anwendung repariert, die Sie in den reparablen Zustand versetzen. Sie können eine Website auswählen, indem Sie auf **Surfen** klicken. Sie können auch nach einer Datei suchen, indem Sie auf **Durchsuchen** klicken.
5. Klicken Sie auf **OK**.
6. Wählen Sie die zu überwachende(n) .EXE/.DLL-Dateien aus. Weitere Informationen finden Sie unter "Auswahl der zu überwachenden Dateien" weiter unten in diesem Kapitel.

Standardmäßig werden ARLs im Verzeichnis \Programme\Intel\DTM\Ldlogon auf dem Core Server gespeichert.

So legen Sie die zu überwachenden Dateien fest

1. Wählen Sie im Fenster "Application Healing" den Namen der Anwendung aus, zur der Sie Dateien hinzufügen möchten.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Dateiliste konfigurieren**.
3. Standardmäßig werden alle .EXE- und .DLL-Dateien ausgewählt. Entfernen Sie aus der Liste alle System- oder freigegebenen .DLLs, die nicht überwacht werden sollen und klicken Sie auf **OK**.
4. Klicken Sie auf **ARL speichern**, um die Änderungen zu speichern.

Informationen zum Dialogfeld "Anwendung zur Anwendungsreparaturliste hinzufügen".

Verwenden Sie das Dialogfeld "Anwendung zu Anwendungsreparaturliste hinzufügen" (Application Healing, Schaltfläche **Anwendung zu Anwendungsreparaturliste hinzufügen** in der Symbolleiste), um die Dateien hinzuzufügen, die Application Healing überwachen soll.

- **Anwendungsname:** Geben Sie den Namen der Anwendung ein, die Sie konfigurieren. Dieser Name wird in der Spalte "Anwendungsreparaturliste" angezeigt.
- **Webpfad:** Klicken Sie auf "Webpfad", um Pakete anzuzeigen, die auf einem Webserver gespeichert sind. Sie müssen http:// in die URL-Angabe mit einschließen.
- **Dateifreigabepfad:** Klicken Sie auf "Dateifreigabepfad", um Pakete anzuzeigen, die in einer Nullsitzungsfreigabe auf einem Dateiserver gespeichert sind. Dieser Pfad muss den UNC-Pfadkonventionen \\servername\freigabename\ entsprechen.
- **Durchsuchen:** Klicken Sie auf **Durchsuchen**, um nach dem Pfad zu suchen. Wenn Sie auf **Webpfad** geklickt haben, wird ein kleines Fenster zum Durchsuchen angezeigt. Wenn Sie auf **Dateifreigabepfad** geklickt haben, wird ein Standarddialogfeld zum Durchsuchen angezeigt.

Organisieren von ARL-Dateien

Sie haben zwei Möglichkeiten bei der Organisation von ARL-Dateien:

- Eine Anwendung pro ARL-Datei
- Mehrere Anwendungen pro ARL-Datei

Wenn Sie eine Anwendung pro ARL-Datei festlegen möchten, verwalten Sie ARLs auf dem Client auf einer Basis, die auf der einzelnen Anwendung beruht. Auf diese Weise haben Sie viele Optionen für das Anpassen von Application Healing auf dem Client. Der Nachteil ist, dass die Verfolgung schwieriger ist, da Clients ein Dutzend oder mehr ARL-Dateien auf ihren Computern gespeichert haben können, abhängig davon, wie viele Anwendungen reparabel sind.

Wenn Sie mehrere Anwendung pro ARL-Datei festlegen möchten, müssen Sie sich überlegen, wie Sie Anwendungen innerhalb einer ARL gruppieren möchten. Sie können z.B. auch eine globale ARL-Liste festlegen, die Anwendungen enthält, die jeder Benutzer in Ihrem Unternehmen ausführt. Jeder erhält diese globale ARL-Datei. Sie benötigen vermutlich auch eine ARL-Datei für die Abteilung, zu der ein Client gehört, z.B. eine Liste für die Buchhaltung, eine für Marketing usw., die die Anwendungen enthält, die spezifisch für diese Abteilung sind.

Vermeiden Sie, dass durch verschiedene Anwendungen in ARL-Dateien auf dieselben .EXE- oder .DLL-Dateien verwiesen wird. Wenn Sie z.B. meinedatei.exe mit zwei verschiedenen Anwendungen in der ARL-Datei verknüpfen, beginnt der Application Healing-Agent mit der Reparatur der ersten Anwendung, die er in einer ARL-Datei mit der zu überwachenden Datei meinedatei.exe findet - unabhängig davon, ob es sich bei dieser Anwendung um die Anwendung mit dem Fehler handelt.

Infos über das Dialogfeld "Mit der Anwendung verknüpfte Dateien"

Verwenden Sie das Dialogfeld "Mit der Anwendung verknüpfte Dateien", um zu konfigurieren, welche Dateien Application Healing auf Probleme hin überwacht.

- **Verfügbare Dateien:** Führt alle .EXE- und .DLL-Dateien im von Ihnen ausgewählten ESWD-Paket auf.
- **Ausgewählte Dateien:** Führt einen Teilsatz der verfügbaren Dateien auf, die Sie überwachen möchten. Sie müssen diese Dateien umsichtig auswählen. Weitere Informationen finden Sie unter "Auswahl der zu überwachenden Dateien" im nächsten Abschnitt.

Auswahl der zu überwachenden Dateien

Der Application Healing-Agent sucht nach Fehlern beim Starten von .EXEs oder Laden von .DLLs. Der Agent protokolliert alle erkannten Fehler in das AMS-Warnprotokoll auf dem Core Server. Wenn eine .EXE- oder .DLL-Datei in einer ARL-Datei ein Problem verursacht, löst der Agent den Reparaturvorgang mithilfe von Informationen in der ARL-Datei aus.

Wenn Sie ein Reparaturpaket in einer ARL-Datei festgelegt haben und auf die Schaltfläche "Anwendungsdateien auswählen" geklickt haben, führt Application Healing die .EXE- und .DLL-Dateien aus dem Paket auf. Wählen Sie die .EXE- und .DLL-Dateien, die den Reparaturvorgang auslösen, mit Umsicht aus; wenn Sie eine .DLL-Datei auswählen, die von mehreren Anwendungen verwendet wird (z.B. MSVC42.DLL), wird möglicherweise die falsche Anwendung repariert, wenn ein Problem vorliegt.

Eine Anwendung kann aus mehreren .EXE- und .DLL-Dateien bestehen; Fehler treten jedoch in der Regel in einem Teilsatz der Dateien auf. Da der Client-Agent Fehler in allen Anwendungen protokolliert, können Sie in den AMS-Protokollen prüfen, wo die Fehler aufgetreten sind. Dies kann ein guter Ausgangspunkt sein für das Kürzen der Liste der .EXE/.DLL-Dateien, die den Reparaturvorgang auslösen. Wählen Sie zunächst zumindest die wichtigste .EXE-Datei aus, auf die die Anwendungsverknüpfung verweist.

In manchen Fällen kann die Auswahl von zu vielen Dateien zu einem anderen Problem führen. Manche Anwendungen versuchen, .DLLs zu laden, die sie nicht benötigen. Eine Anwendung, die unter Windows NT und Windows 98SE ausgeführt wird, kann z.B. nach einer .DLL suchen, die spezifisch für Windows NT ist. Wenn diese .DLL nicht verfügbar ist, geht die Anwendung davon aus, dass sie unter Windows 98SE ausgeführt wird und es kommt zu keinen Problemen. Wenn die Anwendung jedoch nach der .DLL sucht und es sich bei der Komponente, die nach der .DLL sucht, um eine überwachte Datei handelt, wird Application Healing überflüssigerweise gestartet. Wenn Sie feststellen, dass Anwendungen wegen .DLLs fehlschlagen, die nicht zur Anwendung gehören, sollten Sie ggf. die Quell-.DLL aus der Liste der ausgewählten Dateien entfernen.

Wenn eine .EXE- oder .DLL-Datei in mehreren ARL-Dateien festgelegt wurde, verwendet Application Healing die erste gefundene ARL-Datei, die die problematische .EXE/.DLL-Datei aufführt. Vermeiden Sie es, dieselben .EXE/.DLLs in mehreren Anwendungseinträgen zu verwenden.

Konfigurieren von Schritt 3: Bereitstellen von ARL-Dateien auf Clients

Nachdem Sie die ARL mithilfe der Konsole erstellt haben, müssen Sie die ARL auf die Clients verteilen. Der Application Healing-Agent auf dem Client verwendet die ARL-Dateien, um zu bestimmen, welche Anwendungen auf welche Weise reparabel sind. Wenn eine Anwendung nicht mit einer ARL-Datei auf dem Client verknüpft ist, ist die Anwendung nicht reparabel.

So verteilen Sie ARL-Dateien auf Clients

1. Wählen Sie im Fenster "Application Healing" die ARL-Datei aus, die Sie verteilen möchten, und klicken Sie dann auf **Erstellt den geplanten Task**.
2. Das ARL-Dateifeld sollte den ARL-Namen enthalten, den Sie verteilen. Wenn dies nicht der Fall ist, können Sie die ARL-Datei auswählen, indem Sie auf **Auswählen** klicken und eine ARL aus der Liste auswählen.
3. Geben Sie den Skriptnamen an, wie z.B. "Buchhaltungs-ARL bereitstellen". Sie sollten mindestens den Text "ARL" in den Skriptnamen aufnehmen, damit Sie ihn im Fenster "Geplante Tasks" wiederfinden.
4. Klicken Sie auf **OK**, um das Fenster "Geplante Tasks" zu öffnen.
5. Wählen Sie die Computer aus, auf die Sie diese ARL verteilen möchten, indem Sie Clients aus der Netzwerkansicht in das Fenster "Geplante Tasks" ziehen und ablegen.
6. Doppelklicken Sie auf den ARL-Task und legen Sie fest, wann die Verteilung stattfinden soll. Klicken Sie dann auf **OK**.
7. Wiederholen Sie diesen Task für jede einzelne ARL, die Sie verteilen möchten.

Sie können ARL-Dateien auf Clients aktualisieren, indem Sie Änderungen an der entsprechenden ARL vornehmen und sie dann an die Clients neu verteilen.

So entfernen Sie ARL-Dateien von Clients

1. Wählen Sie im Fenster "Application Healing" die ARL-Datei, die Sie entfernen möchten, und klicken Sie dann auf **Erstellt den geplanten Task**.
2. Das ARL-Dateifeld sollte den ARL-Namen enthalten, den Sie entfernen. Wenn dies nicht der Fall ist, können Sie die ARL-Datei auswählen, indem Sie auf **Auswählen** klicken und eine ARL aus der Liste auswählen.
3. Geben Sie den Skriptnamen an, wie z.B. "Buchhaltungs-ARL entfernen". Sie sollten mindestens den ARL-Namen in den Skriptnamen aufnehmen, damit Sie ihn im Fenster "Geplante Tasks" wiederfinden.
4. Klicken Sie auf **Skript entfernen**.
5. Klicken Sie auf **OK**, um das Fenster "Geplante Tasks" zu öffnen.
6. Wählen Sie die Computer aus, von denen Sie diese ARL entfernen möchten, indem Sie Clients aus der Netzwerkansicht in das Fenster "Geplante Tasks" ziehen und ablegen.
7. Doppelklicken Sie auf den ARL-Task und wählen Sie aus, wann die Entfernung stattfinden soll. Klicken Sie dann auf **OK**.
8. Wiederholen Sie diesen Task für jede ARL, die Sie entfernen möchten.

Informationen zum Dialogfeld Anwendungsreparaturlisten (ARL)-Datei planen

Verwenden Sie das Dialogfeld "Anwendungsreparaturlisten (ARL)-Datei planen", um ein Skript zu erstellen, das die ARL auf den Clients bereitstellt.

- **Name der Anwendungsreparaturliste (ARL):** Wählen Sie den ARL-Namen aus, den Sie bereitstellen möchten. Klicken Sie auf "Auswählen", um Ihre Auswahl aus der Liste der verfügbaren ARL-Dateien zu treffen.
- **Name: Geben Sie den Namen für dieses Skript ein.** Dieser Name wird im Fenster "Geplante Tasks" angezeigt.
- **Skript bereitstellen:** Wählen Sie diese Option, um ein ARL-Bereitstellungsskript zu erstellen.
- **Skript entfernen:** Wählen Sie diese Option, um ein Skript zu erstellen, das die festgelegte ARL von den Clients entfernt.

Anzeigen von Application Healing-Ereignissen

Der Application Healing-Agent sendet Alert Management System (AMS)-Ereignisse an den Core Server. Wenn Clients nicht mit dem Netzwerk verbunden sind, speichert der Agent Ereignisse lokal und leitet sie an den Core Server weiter, sobald der Client die Verbindung herstellen kann.

Application Healing speichert Ereignisse sowohl in der AMS-Datenbank als auch in der Core-Datenbank, in der alle Management Suite-Daten gespeichert sind. Ereignisse, die in der Core-Datenbank gespeichert sind, bleiben dort gespeichert, bis Sie sie löschen. Löschen Sie diese Ereignisse in regelmäßigen Abständen aus der Core-Datenbank, indem Sie den weiter unten in diesem Abschnitt beschriebenen Lösch-Task durchführen.

Der Application Healing-Agent sendet diese Ereignisse an den Core Server:

- Die Anwendung wurde nicht repariert. Die Reparatur wurde auf dem Computer deaktiviert.
- Letzte Neuinstallation ist fehlgeschlagen.
- Die Neuinstallation war erfolgreich.
- Die Neuinstallation war erfolgreich, die Anwendung wird neu gestartet.
- Die Reparatur wurde verschoben.
- Die Anwendung wird repariert.
- Die Anwendung kann nicht neu installiert werden.
- Anwendung kann nicht repariert werden.
- Benutzer hat die Reparatur abgebrochen.

Wenn Sie ein Ereignis konfigurieren, das eine Aktionsmeldung verwendet, müssen Sie den Warnparameter <Computername> in <Computer> ändern. Bei Application Healing-Ereignissen ist <Computername> stets der Core Server. <Computer> gibt den Namen des Clients zurück, der ursprünglich das Ereignis generiert hat.

So zeigen Sie Application-Healing-Ereignisse an

- Klicken Sie auf **Ansicht | Warnungsprotokoll**.

So erstellen Sie Alarmaktionen für Application Healing-Ereignisse

1. Klicken Sie auf **Konfigurieren | Alarmeinstellungen**.
2. Erweitern Sie im Fenster "Alarmeinstellungen" den Baum **LANDesk Application Healing** .
3. Doppelklicken Sie auf das Ereignis, für das Sie eine Aktion konfigurieren möchten.
4. Schließen Sie den Assistenten für die Konfiguration von Ereignisaktionen ab.

So löschen Sie Application Healing-Ereignisse aus der Core-Datenbank

1. Klicken Sie im Fenster "Application Healing" auf die Schaltfläche **Healing-Ereignisse löschen**.
2. Wählen Sie aus, ob alle Ereignisse oder nur die Ereignisse gelöscht werden sollen, die älter sind als ein von Ihnen festgelegtes Datum.

Ändern der Verwendung der TCP-Portereignisse

Application Healing verwendet TCP, um Ereignisinformationen zu senden. Standardmäßig ist es für Application Healing erforderlich, dass Port 12175 auf allen Firewalls zwischen Clients und ihrem Core Server geöffnet ist. Wenn Sie einen anderen Port verwenden möchten, können Sie mithilfe des Client-Setup-Assistenten den Standardport ändern, den Application Healing zum Senden von Ereignissen verwendet. Wenn Sie die Clients so konfigurieren, dass sie einen benutzerdefinierten Port verwenden, müssen Sie auch den Core Server so konfigurieren, dass er denselben Port überwacht.

So ändern Sie den TCP-Port, den der Core Server für Ereignisse verwendet

- Ändern Sie auf dem Core Server den Wert für diesen Registrierungsschlüssel, sodass er mit dem Port übereinstimmt, den Ihre Clients verwenden:

  HKLM\Software\Intel\LANDesk\LDWM\QIPSrvr\TCPPort

Anzeigen von Application-Healing-Berichten

Application Healing erstellt verschiedene Berichte, die Sie anzeigen können. Alle Berichte stammen aus der Core-Datenbank.

So zeigen Sie Application-Healing-Bericht an

1. Klicken Sie in der Netzwerkansicht auf **Extras** | **Berichte**.
2. Klicken Sie auf **Alle LDMS-Berichte > Application Healing >** und doppelklicken Sie auf den Bericht, den Sie anzeigen möchten.
3. Klicken Sie ggf. auf den Berichtbereich, den Sie anzeigen möchten.
4. Klicken Sie auf **OK**.

Beschreibungen der einzelnen Berichte finden Sie in den folgenden Abschnitten.

Pro Computer reparierte Anwendungen

Der Bericht "Pro Computer reparierte Anwendungen" führt alle Anwendungen auf, die auf der Basis der einzelnen Clients repariert wurden. Dieser Bericht führt auch Folgendes auf:

- Häufigkeit des Fehlschlagens von Application Healing
- Häufigkeit des Abbrechens von Application Healing
- Häufigkeit der Reparaturen für jede Anwendung
- Datum, an dem die Anwendung zuletzt repariert wurde
- Alle "beschädigten" Anwendungen, die nicht über ein verknüpftes Paket verfügen

Liste "Beschädigte Anwendungen"

Der Listenbericht "Beschädigte Anwendungen" führt alle Dateien auf, die als beschädigt erkannt wurden, jedoch über kein entsprechendes Paket verfügen. Der Bericht führt außerdem auf, wie oft die Anwendung als beschädigt erkannt wurde.

Computer-Ereignisprotokoll

Der Bericht "Computer-Ereignisprotokoll" führt alle Application Healing-Ereignisse auf, die mit einem bestimmten Client verknüpft sind.

Pro Anwendung reparierte Computer

Der Bericht "Pro Anwendung reparierte Computer" führt alle Clients auf, auf denen eine bestimmte Anwendung repariert wurde. Der Bericht enthält außerdem, wie oft die Anwendung erfolgreich repariert wurde und wie oft die Reparatur auf einer Basis pro Client fehlgeschlagen ist.

Application Healing-Registrierungsschlüssel

Die folgenden Registrierungsschlüssel dienen nur der Referenz. Die meisten dieser Schlüssel werden als Ergebnis von Entscheidungen festgelegt, die Sie bei der Installation von Application Healing treffen. Diese Schlüssel müssen nur in sehr wenigen Fällen manuell geändert werden.

Registrierungsschlüssel für die Clientkonfiguration

Der Client-Healing-Agent verwendet den Schlüssel HKLM\Software\Intel\LANDesk\LDWM\QIP zum Speichern der meisten Konfigurationsdaten. Die folgenden Werte werden unterstützt:

Wert	Typ	Beschreibung
ConnectionFreq	DWORD	Wenn der Agent keine anfängliche Verbindung mit dem Core Server herstellen kann, versucht er in regelmäßigen Abständen, diese herzustellen. Dieser Registrierungswert legt fest, wie häufig (in Sekunden) der Verbindungsversuch wiederholt wird. Gültige Werte liegen zwischen 5 und 3600 (ein Mal pro Stunde). Der Standardwert ist 120 Sekunden (2 Minuten).
QueueCompactFreq	DWORD	Häufigkeit der Komprimierung der Warteschlange (in Sekunden). Gültige Werte liegen zwischen 30 und 86400 (ein Mal pro Tag). Der Standardwert ist 900 Sekunden (15 Minuten).
TCPPort	DWORD	Festlegen des TCP-Ports, den der Agent bei der Kommunikation mit dem Server verwendet. Standardmäßig ist dieser Wert 12175. Sie müssen dieselbe Portnummer auf dem Core Server und den Clients verwenden.

Es gibt einen zusätzlichen Schlüssel unter "HKLM\Software\Intel\LANDesk\Metering\Meterwin\Repair". Er unterstützt diesen Wert:

Wert	Typ	Beschreibung
Utility	String	Enthält den Pfad zur Datei SDISTFIX.EXE, der ausführbaren Clientdatei von Application Healing. Standard ist c:\Ldclient\SDISTFIX.EXE. Wenn SDISTFIX.EXE nicht unter C:\ldclient auf den Clients gespeichert ist, müssen Sie diesen Schlüssel so ändern, dass er auf den neuen Speicherort verweist. Andernfalls funktioniert die Reparatur nicht.

Registrierungsschlüssel für den Client-Healing-Agenten

Die Konfigurationsdaten für den Client-Healing-Agenten sind unter dem Schlüssel HKLM\Software\Intel\LANDesk\LDWM\AppHealing\Agent gespeichert. Diese Werte sind unter diesem Schlüssel gespeichert:

Wert	Typ	Beschreibung
DialogTimeOut	DWORD	Die Zeit (in Sekunden) bis zum Timeout des Assistenten für Application Healing; danach wird die Reparatur der Anwendung fortgesetzt. Gültige Werte liegen zwischen 10 und 3600 Sekunden (eine Stunde). Der Standardwert ist 300 Sekunden (5 Minuten).
DisableHealing	DWORD	Wenn dieser Wert auf einen Wert ungleich Null festgelegt ist, wird Application Healing auf dem Client deaktiviert.
MinHealDelta	DWORD	Bestimmt, wie viele Sekunden vergehen müssen, bevor ein weiterer Reparaturversuch unternommen wird. Gültige Werte liegen zwischen 10 und 3600 Sekunden (eine Stunde). Der Standardwert ist 600 Sekunden (10 Minuten).
UIFlags	DWORD	Bitweise Kennzeichnungen, die steuern, wie die Benutzeroberfläche (für sowohl SDISTFIX.EXE- als auch Paketinstallation) angezeigt wird. Die folgenden Optionen sind verfügbar: 0x1000, stille Installation; es wird keine Benutzeroberfläche angezeigt 0x2000, alternativer Paketspeicherort nicht zulässig 0x4000, Benutzer kann die Reparatur nicht bis zur nächsten Anmeldung verschieben 0x0001, Benutzer kann den Vorgang nicht abbrechen 0x0002, es wird kein Hintergrund angezeigt während der Neuinstallation des Pakets. Standardmäßig sind die Bits festgelegt, die keinen Abbruch zulassen und keinen Hintergrund anzeigen (Ox0003).

Registrierungsschlüssel für den Server-Healing-Agenten

Der Server-Healing-Agent verwendet den Schlüssel HKLM\Software\Intel\LANDesk\LDWM\QIPSrvr zum Speichern von Konfigurationsdaten. Die folgenden Werte werden unterstützt:

Wert	Typ	Beschreibung
MaxConnections	DWORD	Steuert die maximale Anzahl von Clients, die mit dem Server-Healing-Agenten verbunden werden können. Gültige Werte liegen zwischen 1 und 32. Standard ist der Wert 32. Hinweis: Jede Verbindung führt zu einem Thread, der im Server-Healing-Agenten erstellt wird.
MaxInactiveLibTime	DWORD	Zielhandler werden dynamisch durch den Server-Healing-Agenten je nach Bedarf geladen. Die Zielhandler werden entladen, wenn sie eine gewisse Zeit inaktiv gewesen sind (d.h. sie haben kein Paket erhalten). Dieser Wert legt die Anzahl der Sekunden fest, die ein Handler inaktiv gewesen sein muss,

		bevor er entladen wird. Dieser Wert wird nicht validiert. Der Standardwert ist 300 Sekunden (5 Minuten).
TCPPort	DWORD	Festlegen des TCP-Ports, den der Server-Healing-Agent bei der Kommunikation mit den Clients verwendet. Standardmäßig ist dieser Wert 12175. Sie müssen dieselbe Portnummer auf dem Core Server und den Clients verwenden.

SDClient-Verzeichnisregistrierungsschlüssel

Standardmäßig nimmt Application Healing an, dass sich die ausführbare Clientdatei von Application Healing (SDISTFIX.EXE) im Verzeichnis C:\Ldclient befindet. Sie können ein anderes Verzeichnis für SDISTFIX.EXE angeben, indem Sie den SDClientDirectory-Wert unter dem Schlüssel HKLM\Software\Intel\LANDesk\LDWM\Distribution festlegen.

Kapitel 11: Verwalten von Anwendungsrichtlinien

LANDesk Management Suite ermöglicht die Verwaltung von Anwendungsgruppen auf mehreren Clients mithilfe der Komponente Application Policy Management.

In diesem Kapitel erfahren Sie mehr über:

- Application Policy Management
- Konfigurieren von Richtlinien
- Auswählen von Zielen für die Richtlinien
- Erläuterungen zu Richtlinientypen
- Erstellen von Berichten über den Richtlinienstatus

Informationen über Application Policy Management

Mit Application Policy Management (APM) können Anwendungsgruppen problemlos auf mehreren Clients verwaltet werden. Eine Richtlinie besteht aus zwei Hauptkomponenten:

- Enhanced Software Distribution (ESWD)-Paketen, die von Ihnen erstellt werden.
- Richtlinienzielen für die ESWD-Pakete, wie die Ergebnisse einer LDAP- oder Core-Datenbankabfrage

Eine der wichtigsten Funktionen von Application Policy Management ist die periodische Wiederholung der Abfragen, die Sie als Teil der Richtlinie definiert haben. Auf diese Weise werden die festgelegten Richtlinien auf alle neuen verwalteten Clients angewendet. Angenommen im LDAP-Verzeichnis gibt es einen Container "Abteilung", der Benutzerobjekte enthält. Alle Benutzer, deren Abteilungsobjekt "Marketing" ist, verwenden die Standardanwendungen. Nachdem Sie eine Richtlinie für die "Marketing"-Benutzer eingerichtet haben, werden auf den Computern der Benutzer, die dem Objekt "Marketing" neu hinzugefügt werden, automatisch die richtigen Anwendungen installiert.

Eine Richtlinie ist im Prinzip eine Befehlszeile für Enhanced Software Distribution (ESWD)-Pakete, die auf Zielclients ausgeführt wird. Mit der LANDesk Management Suite-Konsole können Sie Anwendungsrichtlinien konfigurieren, die in der Core-Datenbank gespeichert sind.

Application Policy Management eignet sich für folgende Dateitypen:

- Enhanced Software Distribution (ESWD)-Pakete
- Microsoft Installer (MSI)-Pakete
- Eigenständige ausführbare Einzeldateien

Im Folgenden wird der Taskfluss für Application Policy Management beschrieben:

1. Stellen Sie sicher, dass sich Application Policy Management- und ESWD-Agenten auf den Clients befinden.
2. Falls für die Anwendung, für die eine Richtlinie verwendet werden soll, kein ESWD-Paket vorhanden ist, müssen Sie eines erstellen. Weitere Informationen finden Sie in Kapitel 6: "Verteilen von Software und Dateien".
3. Verwenden Sie die Konsole zum Konfigurieren der Anwendungsrichtlinien und der Richtlinienziele. In der Core-Datenbank werden Richtlinienziele gespeichert, die als Benutzer-/Computergruppen oder Ergebnisse von LDAP-/Datenbankabfragen definiert werden können.
4. Der Application Policy Management-Dienst auf dem Core Server aktualisiert in regelmäßigen Abständen die Liste der Richtlinienziele durch eine Neubewertung der Ergebnisse von LDAP-/Datenbankabfragen. Dadurch wird sichergestellt, dass die Zielbenutzer/-computer in der Core-Datenbank immer auf dem aktuellen Stand sind.
5. Ein Benutzer meldet sich auf einem Clientcomputer an, stellt eine Verbindung zum Netzwerk her oder startet den Application Policy Management-Agenten auf andere Weise.

6. Der Application Policy Management-Dienst des Core Servers ermittelt die anzuwendenden Richtlinien unter Berücksichtigung der Gerätekennung des Computers und des angemeldeten Benutzers.
7. Der Application Policy Management-Dienst sendet die Richtlinieninformationen zurück an den Application Policy Management-Agenten.
8. Abhängig davon, wie Sie die Richtlinienverarbeitung auf dem Client konfiguriert haben, muss der Benutzer die auszuführenden Richtlinien auswählen, oder die Richtlinien werden automatisch ausgeführt. In der Clientliste stehen nur empfohlene oder optionale Richtlinien zur Verfügung. Wird eine unverarbeitete empfohlene Richtlinie in der Liste angezeigt, so wird sie standardmäßig mit einem Häkchen gekennzeichnet. Periodische Richtlinien werden in der Liste angezeigt, sobald ihre Ausführungsintervalle abgelaufen sind. Ausgewählte Richtlinien werden nacheinander ausgeführt.
9. Der Application Policy Management-Agent sendet die Richtlinienergebnisse an den Core Server, der die Ergebnisse in der Core-Datenbank speichert. Um zuverlässigere Ergebnisse zu erhalten, wird QIP für Application Policy Management-Statusberichte verwendet. Dieser Status wird im dritten Bereich des Application Policy Management-Fensters angezeigt.

Informationen über das Application Policy Management-Fenster

Das Application Policy Management-Fenster ist in drei Bereiche unterteilt:

- Im ersten Bereich werden Name und Pakettyp der Richtlinie angezeigt.
- Im zweiten (mittleren) Bereich werden die Gruppen angezeigt, die Zielclients für diese Richtlinie enthalten. Außerdem wird angezeigt, wie häufig die Richtlinie von Application Policy Management angewendet wird.
- Der dritte Bereich enthält weitere Informationen zu den Zielclients der in der mittleren Spalte ausgewählten Gruppe. Darüber hinaus wird der Status der Richtlinie für den Client angezeigt und wann der Status zuletzt aktualisiert wurde.

Konfigurieren von Richtlinien

Bevor Sie Richtlinien erstellen, müssen Sie sicherstellen, dass der Application Policy Management-Agent auf den Clients bereitgestellt wurde.

Application Policy Management benötigt ESWD-Pakete für alle erstellten Richtlinien. Die ESWD-Pakete können entweder im Voraus oder beim Erstellen der Richtlinie erstellt werden. Sie sollten die Pakete im Voraus erstellen, damit Sie sie testen können, bevor sie für eine Richtlinie verwendet werden.

So erstellen Sie eine Richtlinie

1. Klicken Sie in der Konsole auf **Extras | Application Policy Management**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Richtlinie hinzufügen**.
3. Geben Sie im Fenster "Paket bereitstellen" den **Webpfad** oder **Dateifreigabepfad** des Pakets an oder klicken Sie auf **Durchsuchen**, um ein bereits erstelltes Paket auszuwählen.
4. Führen Sie die restlichen Anweisungen des Assistenten aus. Klicken Sie auf **Hilfe**, um weitere Informationen zu den einzelnen Seiten abzurufen.
5. Fügen Sie Ziele für die Richtlinie hinzu. Nähere Informationen hierzu finden Sie im nächsten Abschnitt.

Auswählen von Zielen für die Richtlinien

Sie müssen für jede erstellte Richtlinie eine Gruppe von Zielen angeben, auf die Application Policy Management die Richtlinie anwenden soll. Application Policy Management kennt zwei Typen von Zielen: statische und dynamische.

- **Statische Ziele:** Eine Liste bestimmter Geräte oder Benutzer, die ausschließlich manuell geändert werden kann. Statische Ziele können im Directory Manager ausgewählte Benutzer oder in der Netzwerkansicht der Konsole ausgewählte Geräte sein.
- **Dynamische Ziele:** Eine dynamische Liste mit Geräten, anhand derer Application Policy Management die aufgelisteten Geräte auf Änderungen hin überprüfen kann. Zu dynamischen Zielen gehören Abfrageergebnisse, LDAP-Gruppen/-Container und Gruppen in der Netzwerkansicht.

Dynamische Richtlinienziele sind insofern einmalig, als Management Suite die Ergebnisse dieser Abfragen periodisch aktualisiert. Wenn neue Clients die Abfragekriterien erfüllen, werden Richtlinien, die diese Abfragen verwenden, auf die neuen Clients angewendet.

Es gibt folgende Möglichkeiten, statische Richtlinienziele anzugeben:

- **Computer in der Netzwerkansicht:** Eine statische Gruppe von Computern aus der Core-Datenbank.
- **LDAP-Benutzer oder Rechner::** Eine statische Gruppe von Benutzer- und/oder Rechnerobjekten.

Es gibt folgende Möglichkeiten, dynamische Richtlinienziele anzugeben:

- **Gruppe in der Netzwerkansicht:** Eine dynamische Gruppe von Computern aus der Core-Datenbank.
- **LDAP-Gruppe / -Container:** Eine dynamische Gruppe von Benutzer- und/oder Rechnerobjekten.
- **Datenbankabfrage:** Eine Gruppe von Computern, die mithilfe einer Abfrage der Core-Datenbank generiert wird..
- **Benutzergruppe:** Eine Gruppe von Benutzern, die aus einem LDAP-kompatiblen Verzeichnis ausgewählt wird.
- **LDAP-Abfrage:** Eine Gruppe von Benutzern, Computern oder beidem, die mithilfe einer Abfrage eines LDAP-kompatiblen Verzeichnisses generiert wird.

Hinzufügen statischer Ziele

Application Policy Management kann statische Ziele als Richtlinienziele verwenden. Statische Ziele sind eine Liste bestimmter Geräte oder Benutzer, die ausschließlich manuell geändert werden kann.

So fügen Sie statische Ziele aus der Netzwerkansicht hinzu

- Wählen Sie in der Netzwerkansicht einzelne Clients aus und ziehen Sie sie in den mittleren Fensterbereich.

So fügen Sie statische Ziele aus Directory Manager hinzu

- Ziehen Sie Objekte von Directory Manager in den mittleren Bereich des Application Policy Management-Fensters.

So fügen Sie ein statisches Ziel manuell hinzu

1. Klicken Sie im Kontextmenü des Zielbereichs auf **Neues statisches Ziel**.
2. Geben Sie die Daten zum Ziel in das Dialogfeld "Neues statisches Ziel" ein.
3. Ziehen Sie Ziele aus der Netzwerkansicht oder dem Directory Manager.

Hinzufügen dynamischer Ziele

Application Policy Management kann Richtlinienziele mithilfe von Abfragen ermitteln. In Management Suite 8 werden Abfragen lediglich in der Core-Datenbank gespeichert. Weitere Informationen zu Abfragen finden Sie in Kapitel 4 "Verwalten von Inventar und Berichten".

Wenn Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf eine Abfrage klicken, können Sie überprüfen, ob der ausgewählten Abfrage Anwendungsrichtlinien zugeordnet sind.

Damit Clients Richtlinien empfangen können, die über Active Directory- oder NetWare-Verzeichnisdienste angegeben werden, muss für sie die Anmeldung beim Verzeichnis konfiguriert werden. Das bedeutet, dass die richtige Clientsoftware installiert sein muss. Außerdem müssen sich die Clients beim richtigen Verzeichnis anmelden, damit ihr eindeutiger, definierter Name dem Namen entspricht, der über Directory Manager und Application Policy Manager angegeben wurde.

Windows 95/98-Clients müssen so konfiguriert sein, dass ihre Anmeldung bei der Domäne erfolgt, die Active Directory enthält. Active Directory wird von Windows NT und Windows 95/98 nicht unterstützt. Sie müssen auf den Clients, die sich bei einem Verzeichnis anmelden und Application Policy Management erfordern, Active Directory-Unterstützung installieren. Zum Zeitpunkt der Veröffentlichung waren unter folgender Adresse weitere Informationen zur Active Directory-Clientunterstützung erhältlich:

http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp

Für jeden Windows NT/2000/2003/XP--Client muss ein Computerkonto auf dem Active Directory-Domänencontroller vorhanden sein. Das bedeutet, der als Client verwendete Computer muss bei der Domäne angemeldet sein, in der Active Directory gespeichert ist. Sie können nicht einfach ein Netzlaufwerk mit dem voll qualifizierten Windows NT-Domänennamen verbinden. Die Richtlinie wird in diesem Fall nicht angewendet.

So verwenden Sie Directory Manager zum Erstellen einer Abfrage

1. Klicken Sie auf **Extras | Directory Manager**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Verzeichnis verwalten**.
3. Geben Sie den Verzeichnis-URL und Authentifizierungs-Informationen ein und klicken Sie auf **OK**.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Abfrage**.
5. Erstellen Sie die Abfrage. Weitere Informationen finden Sie unter "Verwenden von Directory Manager für die Abfrage von Verzeichnissen über LDAP" in Kapitel 3.

So betrachten Sie eine Vorschau der Abfrageergebnisse

- Klicken Sie im mittleren Fensterbereich mit der rechten Maustaste auf eine Gruppe und klicken Sie auf **Abfrageergebnisse-Vorschau**. Beachten Sie, dass die Bearbeitung mancher Abfragen lange dauern kann. Sobald die Abfrage fertiggestellt ist, werden die Ergebnisse im rechten Fensterbereich angezeigt.

So fügen Sie dynamische Ziele aus der Netzwerkansicht hinzu

- Verschieben Sie eine Gerätegruppe mittels Ziehen und Ablegen aus der Netzwerkansicht in den mittleren Bereich des Application Policy Management-Fensters.

So fügen Sie dynamische Ziele aus Directory Manager hinzu

1. Ziehen Sie einen Container oder eine Gruppe aus Directory Manager in den mittleren Bereich des Application Policy Management-Fensters.
2. Wenn Sie einen Container hinzufügen, geben Sie an, ob Benutzerobjekte, Rechnerobjekte oder beides aus dem Container hinzugefügt werden sollen.

So fügen Sie einer Richtlinie mittels einer Abfrage Ziele hinzu

- Verschieben Sie eine Abfrage mittels Ziehen und Ablegen von der Netzwerkansicht in den mittleren Bereich des Application Policy Management-Fensters.

So überprüfen Sie, ob eine Abfrage von einer Richtlinie verwendet wird

- Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf die Abfrage, die überprüft werden soll, und klicken Sie auf **Richtlinien**.

  Oder
- Wählen Sie die Abfrage in Directory Manager aus, um deren Zielrichtlinien im rechten Bereich anzuzeigen.

Kopieren von Zielen in eine andere Richtlinie

Bei komplexen Netzwerk- oder Organisationsstrukturen kann es sehr aufwändig sein, einer Richtlinie Ziele zuzuweisen. Wenn Sie bereits Richtlinienziele konfiguriert haben, können Sie bei weiteren Richtlinien, die dieselben Ziele verwenden, viel Zeit sparen, indem Sie diese Ziele in die neue Richtlinie kopieren.

So kopieren Sie Ziele in eine andere Richtlinie

1. Klicken Sie im Zielbereich auf die Zielliste, die kopiert werden soll. Klicken Sie im Kontextmenü der Zielliste auf **Ziel in andere Richtlinie kopieren**.
2. Klicken Sie auf die Richtlinie, welche die Zielliste erhalten soll, und klicken Sie auf **Verknüpfen**. Klicken Sie auf **Schließen**, wenn Sie fertig sind.

Anwenden von Bereichen auf APM-Richtlinien

Mehrere Bereiche können den APM-Zielfensterausschnitt "Details" filtern, um eine Zielliste zu erhalten. Der letzte Bereich, den eine Richtlinie verwendet, ist jedoch immer der Bereich eines Ziellistenerstellers. Wenn ein Benutzer der Management Suite mit einem anderen Bereich den Zielfensterausschnitt "Details" anzeigt, der durch einen anderen Benutzer erstellt wurde (wir nennen diese zweite Person "Editor" einer Zielliste), wird der Zielfensterausschnitt "Details" zuerst durch den Bereich des Erstellers und dann durch den Bereich des Editors gefiltert. In diesem Fall sieht der Editor möglicherweise nicht alle Ziele im Zielfensterausschnitt "Details", auf die die Richtlinie angewendet wird, da es ihm sein Bereich nicht erlaubt, alle Ziele im Bereich des Erstellers anzuzeigen.

Erläuterungen zu Richtlinientypen

Mit dem Richtlinientyp wird festgelegt, wie sich Zielclients verhalten, wenn sie die Richtlinie empfangen:

- **Erforderlich:** Der Application Policy Management-Agent wendet automatisch die erforderlichen Richtlinien an, ohne dass der Benutzer eingreifen muss. Sie können festlegen, dass erforderliche Richtlinien im Hintergrund ausgeführt werden. Benutzeroberflächen, die während der Installation eines erforderlichen Tasks auf dem Client angezeigt werden, dürfen nicht blockieren. Das heißt, für die Installation der Anwendung darf keine Benutzereingabe erforderlich sein.
- **Empfohlen:** Benutzer können selbst entscheiden, wann empfohlene Richtlinien installiert werden. Empfohlene Richtlinien werden standardmäßig auf der Benutzeroberfläche des Clients ausgewählt.
- **Optional:** Benutzer können selbst entscheiden, wann optionale Richtlinien installiert werden. Optionale Richtlinien werden nicht standardmäßig auf der Benutzeroberfläche des Clients ausgewählt.

Sie können auch konfigurieren, wie häufig eine Richtlinie ausgeführt werden kann.

- **Einmal:** Sobald eine Richtlinie erfolgreich auf einem Client ausgeführt wurde, wird sie von diesem Client nicht mehr ausgeführt.
- **Periodisch:** Wenn eine empfohlene oder optionale Richtlinie als periodisch definiert wird, wird sie von der Benutzeroberfläche entfernt, sobald sie erfolgreich verarbeitet wurde. Sie wird wieder auf der Benutzeroberfläche angezeigt, nachdem das angegebene Intervall abgelaufen ist.
- **Wie gewünscht:** Kann jederzeit vom Benutzer installiert werden.

Was Clients auf ihren Computern sehen

Anwendungsrichtlinien werden immer mit einem Pull-Modell verarbeitet. Clients überprüfen auf dem Core Server, ob neue Richtlinien für sie vorhanden sind. Bei dieser Überprüfung wird beim Client ein Dialogfeld angezeigt, in dem nur unverarbeitete empfohlene und optionale Richtlinien angezeigt werden. Erforderliche Richtlinien werden nicht angezeigt. Wird eine unverarbeitete empfohlene Richtlinie auf der Benutzeroberfläche angezeigt, so wird sie standardmäßig mit einem Häkchen gekennzeichnet, um den Benutzer zu veranlassen, sie zu verarbeiten.

Nachdem eine Richtlinie verarbeitet wurde, wird sie unter Umständen weiterhin auf der Benutzeroberfläche angezeigt wird, sofern sie periodisch ausgeführt wird. In diesem Fall bleibt sie ausgewählt, selbst wenn es sich um eine empfohlene Richtlinie handelt. Eine Richtlinie wird auch dann weiterhin auf der Benutzeroberfläche angezeigt, wenn sie nicht richtig angewendet wurde.

Konfigurieren von Richtlinien auf Macintosh-Clients

Sie können auch Macintosh-Clientrichtlinien erstellen (nur Mac OS X). Das Erstellen einer Macintosh-Clientrichtlinie ähnelt dem Erstellen einer Richtlinie für Windows-basierte Clients. Für Macintosh-Clients sind dieselben Typen erforderlicher, empfohlener und optionaler Richtlinien verfügbar. Macintosh-Anwendungspakete müssen als einzelne Datei vorliegen. Application Policy Management prüft bei der Anmeldung und der Reaktivierung, ob Anwendungsrichtlinien-Aktualisierungen vorhanden sind. Bei der Bestimmung von Richtlinien unterstützt Mac gegenwärtig Application Policy Management nicht nach Benutzernamen, sondern nur nach Rechnernamen.

Application Policy Management nimmt für Macintosh-Anwendungsrichtlinienpakete die folgenden Maßnahmen vor:

1. Herunterladen von Dateien in /Library/Applications/LANDesk/sdcache (entspricht CBA-Downloads).
2. Wenn die heruntergeladenen Dateien komprimiert sind, dekomprimiert Application Policy Management sie im Speicherort.
3. Wenn es sich bei den heruntergeladenen Dateien um ein Festplattenabbild handelt, wird es durch Application Policy Management bereitgestellt.
4. Wenn für die Richtlinie eine Befehlszeile vorhanden ist, wird sie durch Application Policy Management ausgeführt.
5. Wenn die heruntergeladene Datei eine Apple Package Installer-Datei ist, wird sie durch Application Policy Management still ausgeführt.
6. Wenn es sich bei der heruntergeladenen Datei um ein Festplattenabbild handelt, sucht Application Policy Management nach der ersten Apple Package Installer-Datei auf dem bereitgestellten Datenträger und führt sie still aus.
7. Wenn es sich bei den heruntergeladenen Dateien um ein Festplattenabbild handelt, wird es durch Application Policy Management bereitgestellt.

Außerdem unterstützt Application Policy Management .dmg-Dateien mit EULAs.

HINWEIS: Manche Pakettypen funktionieren nicht einwandfrei mit Application Policy Management
Installer Vise- und Installer Maker-Installationen funktionieren in der Regel nicht einwandfrei mit APM. Sie bedürfen fast immer der Benutzerinteraktion und können abgebrochen werden.

So fügen Sie eine Macintosh-Clientrichtlinie hinzu

- Klicken Sie im Fenster "Application Policy Management" auf die Schaltfläche **Neue Macintosh-Richtlinie hinzufügen** und beenden Sie den Assistenten.

So bearbeiten Sie die Befehlszeile eines Macintosh-Richtlinienpakets

1. Doppelklicken Sie im Fenster "Application Policy Management" auf die Richtlinie, die Sie bearbeiten möchten.

2. Fügen Sie Befehlszeilenparameter hinzu, die in der **Richtlinien-Befehlszeile** enthalten sein sollen. Diese Parameter werden an das Paket übergeben.

So aktualisieren Sie lokale Clientrichtlinien

1. Klicken Sie auf dem Macintosh-Client im Fensterausschnitt "Management Suite-Einstellungen" auf die Registerkarte **Übersicht**.
2. Klicken Sie auf **Jetzt prüfen**, um Application Policy Management zu überprüfen.

So zeigen Sie installierte Richtlinien an

- Klicken Sie im Fensterbereich "Management Suite-Einstellungen" auf dem Macintosh-Client auf das Register **APM**.

Erstellen von Berichten über den Richtlinienstatus

Immer, wenn ein Client eine Richtlinie verarbeitet, sendet der Application Policy Management-Agent Statusinformationen zurück an den Core Server. Application Policy Management speichert Statusinformationen in der Core-Datenbank und zeigt sie neben den einzelnen Zielen an.

Application Policy Management unterstützt vier Berichtsarten:

- **APM-Status nach Rechner:**Zeigt Informationen zum Richtlinienstatus für einen ausgewählten Client an. Wenn mehrere Benutzer Richtlinien auf dem Client verarbeitet haben, werden Informationen für alle Benutzer des Clients angezeigt.
- **APM-Status nach Richtlinie:**Zeigt Statusinformationen für eine ausgewählte Richtlinie an.
- **APM-Status nach Benutzer:**Zeigt Informationen zum Richtlinienstatus für einen ausgewählten Benutzer an. Wenn ein Benutzer auf mehreren Clients Richtlinien verarbeitet hat, enthält der Bericht Informationen für alle Clients, auf denen der Benutzer Richtlinien verarbeitet hat.
- **APM-Status aller Richtlinien:**Zeigt Statusinformationen für alle Richtlinien an.

So erzeugen Sie einen Application Policy Management-Bericht

1. Klicken Sie auf **Extras | Berichte**.
2. Klicken Sie im Fenster "Berichte" auf **Alle LDMS-Berichte > APM-Status** und doppelklicken Sie auf den Application Policy Management-Bericht, der generiert werden soll.

So exportieren Sie einen Richtlinienstatus

- Generieren Sie einen Bericht und klicken Sie in der Berichtsansicht auf die Schaltfläche **Bericht exportieren**, um den Bericht zu exportieren.

Informationen über das Dialogfeld Neues statisches Ziel

Im Dialogfeld "Neues statisches Ziel" (zum Öffnen klicken Sie im Kontextmenü des Zielbereichs auf **Neues statisches Ziel**) können Sie einer Richtlinie bestimmte Geräte und Benutzer hinzufügen.

- **Zielname:** Geben Sie einen Namen ein, der dieses Ziel beschreibt.
- **Ziele:** Sie können entweder "Geräte" oder "Benutzer" als Ziele angeben. Wenn Sie "Geräte" auswählen, können Ziele aus der Netzwerkansicht hinzugefügt werden. Wenn Sie "Benutzer" auswählen, können Ziele aus Directory Manager (Extras | Directory Manager) hinzugefügt werden.

- **Erforderlich:** Der Application Policy Management-Agent wendet automatisch die erforderlichen Richtlinien an, ohne dass der Benutzer eingreifen muss. Sie können festlegen, dass erforderliche Richtlinien im Hintergrund ausgeführt werden. Benutzeroberflächen, die während der Installation eines erforderlichen Tasks auf dem Client angezeigt werden, dürfen nicht blockieren. Das heißt, für die Installation der Anwendung darf keine Benutzereingabe erforderlich sein.
- **Empfohlen:** Benutzer können selbst entscheiden, wann empfohlene Richtlinien installiert werden. Empfohlene Richtlinien werden standardmäßig auf der Benutzeroberfläche des Clients ausgewählt.
- **Optional:** Benutzer können selbst entscheiden, wann optionale Richtlinien installiert werden. Optionale Richtlinien werden nicht standardmäßig auf der Benutzeroberfläche des Clients ausgewählt.
- **Einmal:** Sobald eine Richtlinie erfolgreich auf einem Client ausgeführt wurde, wird sie von diesem Client nicht mehr ausgeführt.
- **Wie gewünscht:** Kann jederzeit vom Benutzer installiert werden.
- **Periodisch:**Wenn eine empfohlene oder optionale Richtlinie als periodisch definiert wird, wird sie von der Benutzeroberfläche entfernt, sobald sie erfolgreich verarbeitet wurde. Sie wird wieder auf der Benutzeroberfläche angezeigt, nachdem das angegebene Intervall abgelaufen ist.

Kapitel 12: Konfiguration von Alarmen zu Ihrer Benachrichtigung

LANDesk Alert Management System (AMS) automatisiert Aktionen als Reaktion auf Alarme, die im Netzwerk ausgelöst werden. AMS überwacht Management Suite-Komponenten und -Clients auf das Auftreten bestimmter Ereignisse hin. Wenn diese Ereignisse eintreten, sendet die Komponente oder der Client eine Alarmmeldung an AMS.

Sie können von AMS durch die Ausführung der von Ihnen konfigurierten Alarmaktionen über den Alarm benachrichtigt werden. Beispielsweise können Sie die Konsole so konfigurieren, dass Sie benachrichtigt werden, sobald jemand eine Fernsteuerungssitzung einzurichten versucht. Wenn dieses Ereignis eintritt, erkennt AMS den Versuch und führt die konfigurierten Alarmaktionen aus, sendet z. B. eine Nachricht per Internet-Mail oder Pager.

In diesem Kapitel erfahren Sie mehr über:

- Funktionsweise der Alarmfunktion in Management Suite
- Konfigurieren von AMS-Alarmaktionen
- Konfigurieren der Alarmaktion "Meldungsfeld"
- Konfigurieren der Alarmaktion "Broadcast"
- Konfigurieren der Alarmaktion "Internet-Mail senden"
- Konfigurieren der Alarmaktion "Programm ausführen"
- Konfigurieren der Alarmaktion "In Ereignisprotokoll schreiben"
- Konfigurieren der Alarmaktion "NLM laden"
- Konfigurieren der Alarmaktion "Seite senden"
- Konfigurieren der Alarmaktion "SNMP-Trap senden"
- Arbeiten mit konfigurierten Alarmaktionen
- Anzeigen des AMS-Warnungsprotokolls

Funktionsweise der Alarmfunktion in Management Suite

Sie können AMS so konfigurieren, dass Sie über das Eintreten bestimmter Management Suite-Ereignisse benachrichtigt werden. Beispielsweise können Sie eine Alarmaktion konfigurieren, sodass ein Meldungsfeld auf Ihrem Client angezeigt wird, wenn ein Softwareverteilungspaket bei einem Client nicht ankommt. Falls das betreffende Paket nicht ankommt, erzeugt AMS einen Alarm und zeigt das Meldungsfeld auf Ihrem Client an. Die Konsole ermöglicht die Konfiguration von Alarmen, die durch die Erfüllung bestimmter Parameter ausgelöst werden.

Wenn die festgelegte Alarmbedingung erfüllt ist, sendet die Konsole einen Alarm an AMS. AMS benachrichtigt Sie durch die Ausführung der Alarmaktionen, die Sie im Dialogfeld "Alarmeinstellungen" konfiguriert haben. Folgende Alarmaktionen sind verfügbar:

- Anzeigen eines Meldungsfelds
- Senden von Meldungen durch Broadcasts
- Senden von Internet-E-Mail
- Laden eines NLM
- Ausführen eines Programms
- Speichern von Angaben zu den Ereignissen in einem Ereignisprotokoll
- Senden einer Pager-Nachricht
- Senden einer SNMP Trap-Nachricht

Sie können auch Alarme für NetWare- und Windows 95/98/NT/2000/2003- und Windows XP Professional-Clients konfigurieren. Überdies können Sie den Client auswählen, auf dem die Alarmaktion ausgeführt wird.

Beispielsweise können Sie eine Alarmaktion konfigurieren, sodass ein Meldungsfeld auf Ihrem Client angezeigt wird, wenn ein Softwareverteilungspaket bei einem Client nicht ankommt. Falls das betreffende Paket nicht ankommt, erzeugt AMS einen Alarm und zeigt das Meldungsfeld auf Ihrem Client an.

Die Alarmaktionen, die Sie an einer Konsole konfigurieren, sind an einer anderen Konsole nicht verfügbar. Sie können konfigurierte Alarme in andere Konsolen exportieren, damit Sie auf mehreren Clients dieselben konfigurierten Alarmaktionen verwenden können. Nähere Informationen finden Sie unter "Exportieren von Alarmaktionen in andere Computer" weiter unten in diesem Kapitel.

Konfigurieren von AMS-Alarmaktionen

Im Dialogfeld "Alarmeinstellungen" können Sie Alarme auswählen und Alarmaktionen konfigurieren. Das Dialogfeld "Alarmeinstellungen" enthält eine Ordnerstrukturansicht aller Ereignisse, die von AMS überwacht werden können. Sie können die Ordner erweitern und zusammenfassen, um die darin enthaltenen Ereignisse zu betrachten. Zudem können Sie Alarmaktionen konfigurieren, die ausgeführt werden, sobald AMS eines dieser Ereignisse erkennt.

Konfigurieren von Alarmaktionsmeldungen

Diese Alarmaktionen können Meldungen erzeugen, wenn sie übermittelt werden.

- Meldungsfeld
- Broadcast
- Seite senden
- Internet-Mail senden
- SNMP-Trap senden
- In Ereignisprotokoll schreiben

Diese Meldung kann beliebigen von Ihnen hinzugefügten Text und Informationen über den Alarm enthalten, der die Meldung erzeugt hat. In der folgenden Tabelle sind die Standardparameter verzeichnet, die für alle Meldungen verfügbar sind:

Standardparameter	Beschreibung
Hostname	Name des Hostclients
Datum	Datum, an dem der Alarm ausgelöst wurde
Uhrzeit	Uhrzeit, zu der der Alarm ausgelöst wurde
Alarmname	Name des ausgewählten Alarms
Benutzername	Name des Benutzers, der den Alarm ausgelöst hat (sofern verfügbar)
Beschreibung	Beschreibung des ausgelösten Alarms
Schweregrad	Der Schweregrad des Alarms

Abhängig vom gewählten Alarm, können weitere Parameter verfügbar sein. Das Dialogfeld "Meldung" enthält zwei Listenfelder: Das Feld "Meldung" enthält den Text der Meldung, der übermittelt werden soll. Das Listenfeld "Alarmparameter" enthält die Parameter, die in den Meldungstext aufgenommen werden sollen.

Jeder Parameterplatzhalter, den Sie in das Feld "Meldung" einfügen, wird durch die entsprechende Alarminformation ersetzt, wenn der Alarm ausgelöst wird. Die Alarmgröße ist auf maximal 1 KB beschränkt. Wenn ein Alarm größer als 1 KB ist, kann er nicht zugestellt werden. In einem solchen Fall löst AMS einen Standardalarm aus, um Sie darüber zu benachrichtigen, dass eine Meldung nicht gesendet wurde. Sie können die Alarmaktionen für den Standardalarm konfigurieren, um sicherzustellen, dass Sie darüber informiert werden, wenn eine Meldung nicht zugestellt wird.

Sie können die eingestellten Alarmaktionen testen, um zu überprüfen, ob sie das erwartete Verhalten zeigen. Nähere Informationen hierzu finden Sie unter Testen konfigurierter Alarmaktionen weiter unten in diesem Kapitel.

Konfigurieren von Alarmaktionen

Zur Konfiguration der meisten AMS-Alarmaktionen mit dem Assistent zum Konfigurieren von Alarmen sind ähnliche Schritte auszuführen. Genauere Informationen zum Konfigurieren der verschiedenen Arten von Alarmaktionen finden Sie im betreffenden Abschnitt weiter unten in diesem Kapitel.

So konfigurieren Sie eine Alarmaktion

1. Klicken Sie in der Konsole auf **Konfigurieren | Alarmeinstellungen**.
2. Wählen Sie im Fenster "Alarmeinstellungen" den **Alarm** aus, für den Sie Alarmaktionen konfigurieren möchten.
3. Klicken Sie mit der rechten Maustaste auf den **Alarm** und klicken Sie dann auf **Konfigurieren**.
4. Wählen Sie eine **Alarmaktion** aus und klicken Sie auf **Weiter**.
5. Wählen Sie den **Client** aus, auf dem die Aktion ausgeführt werden soll, und klicken Sie dann auf **Weiter**.
6. Wählen Sie einen **Schweregrad für die Alarmaktion** aus oder verwenden Sie die Voreinstellung. Sie können Alarme so konfigurieren, dass ein wichtiger Alarm als solcher gekennzeichnet wird. Andere weniger wichtige Alarme können Sie der Informations- oder Überwachungsebene zuordnen. AMS verfügt über sechs Schweregrade:
    - Monitor
    - Information
    - OK
    - Kritisch
    - Nicht-kritisch
    - Nicht-wiederherstellbar
7. Klicken Sie auf **Weiter**.
8. Wählen Sie **Details** für die gewählte Alarmaktion aus und klicken Sie dann auf **Weiter**.
9. Falls die Alarmaktion einen Meldungstext senden kann, geben Sie den **Meldungstext** ein, der angezeigt werden soll, in das Feld "Meldung" ein und verschieben Sie die verfügbaren Parameter, die Sie einsetzen möchten, in das Feld "Meldung".

10. Geben Sie einen **Konfigurationsnamen** ein. Dieser Name und der Name des Computers, auf diem die Aktion ausgeführt wird, werden im Dialogfeld "Alarmeinstellungen" neben der zugehörigen Aktion angezeigt.
11. Klicken Sie auf **Fertigstellen**.

Konfigurieren verschiedener Alarmtypen
Detaillierte Angaben zum Konfigurieren der einzelnen Alarmtypen finden Sie in dem Abschnitt zur betreffenden Alarmaktion weiter unten in diesem Kapitel.

Konfigurieren der Alarmaktion "Meldungsfeld"

Mit der Alarmaktion "Meldungsfeld" wird auf dem Client, auf dem Sie die Aktion konfigurieren, ein Meldungsfeld angezeigt. Bei diesem Alarmtyp sind zwei Optionen verfügbar. Sie können:

- **Signalton, wenn angezeigt** - Es ertönt ein Signalton, wenn das Meldungsfeld auf dem Client angezeigt wird.
- **Meldungsfeld systemabhängig** - Ein systemabhängiges Meldungsfeld hindert Sie daran, mit anderen Programmen zu arbeiten, solange Sie das Dialogfeld nicht durch Anklicken bestätigt haben.

Konfigurieren der Alarmaktion "Broadcast"

Mit dieser Alarmaktion wird eine Broadcast-Meldung an jeden gesendet, der mit dem Server verbunden ist, welcher den Alarm erzeugt. Mithilfe der Optionen für "Erweiterte Erkennung" können Sie diesen Alarm so konfigurieren, dass er nur an bestimmte Netzwerksegmente gesendet wird. Nähere Informationen hierzu finden Sie im Abschnitt "Erweiterte Erkennung" der Online-Hilfe.

Die Broadcast-Alarmaktion ist nur in den folgenden Fällen erfolgreich:

1. Der Client, der die Meldung erhält, hat eine Verbindung zum Core Server, wie z.B. ein zugewiesenes Laufwerk.
2. Der Client gehört derselben Domäne und demselben Netzwerksubnetz wie der Core Server an.
3. Der Client ist für den Empfang von Broadcast-Meldungen eingerichtet (unter Windows 2000/2003/XP muss der Messenger-Dienst ausgeführt werden).

Konfigurieren der Alarmaktion "Internet-Mail senden"

Mit dieser Alarmaktion wird eine Internet-Mail-Nachricht an den von Ihnen angegebenen Benutzer gesendet. Sie müssen beim Einsatz der Alarmaktion "Internet-Mail senden" auch den SMTP-Internet-Mailserver angeben, über den die Alarmaktion die Nachricht senden soll.

Wenn Sie den Namen des Mailservers angeben, muss im Netzwerk ein DNS-Server konfiguriert sein, damit die Alarmaktion "Internet-Mail senden" die IP-Adresse des Servers ermitteln kann. Falls kein DNS-Server vorhanden ist, geben Sie die IP-Adresse des Mailservers an.

Diese Alarmaktion funktioniert nur, wenn Sie an Ihrem Standort Zugriff auf einen SMTP-Internet-Mailserver haben.

Konfigurieren der Alarmaktion "Programm ausführen"

Mit dieser Alarmaktion wird auf dem von Ihnen ausgewählten Client ein Programm ausgeführt. Wenn Sie ein Windows-Programm ausführen lassen, stehen die folgenden Fensterzustände zur Auswahl:

- Normal
- Minimiert
- Maximiert

Die Option zur Bestimmung des Fensterzustands hat auf DOS-Programme keinen Einfluss. Geben Sie den vollständigen Pfad und die Befehlszeile für das auszuführende Programm ein. Sie können im Feld "Befehlszeile" beliebige Befehlszeilenoptionen für das auszuführende Programm angeben.

Konfigurieren der Alarmaktion "In Ereignisprotokoll schreiben"

Mit der Alarmaktion "In Ereignisprotokoll schreiben" wird ein Eintrag im Anwendungsprotokoll der Ereignisanzeige von Windows NT erstellt. Dieser Eintrag wird auf dem Client protokolliert, von dem der Alarm gesendet wurde. Diese Alarmaktionen ist nur auf Windows NT-Clients verfügbar.

Konfigurieren der Alarmaktion "NLM laden"

Mit dieser Alarmaktion wird auf einem ausgewählten NetWare-Server ein NLM geladen, sobald der AMS-Alarm ausgelöst wird. Sie müssen durch die Konfiguration dieses Alarms festlegen, welcher NLM auf welchem Server geladen werden soll. Diese Alarmaktion ähnelt der Alarmaktion "Programm ausführen" für Windows NT-Clients.

Wenn Sie diese Aktion zum ersten Mal konfigurieren, sucht AMS im Netzwerk nach NetWare-Clients, die diese Aktion ausführen können.

Geben Sie den zu ladenden NLM in das NLM-Feld ein. NLMs werden auf NetWare-Servern für gewöhnlich im Verzeichnis SYS:SYSTEM gespeichert. Achten Sie darauf, dass Sie den NLM-Pfad angeben, der auf dem betreffenden NetWare-Server gilt. Geben Sie beispielsweise den Systempfad in der Form SYS:SYSTEM\TEST.NLM an. Verwenden Sie keine Laufwerkbuchstabenzuordnungen des Clients wie T:\SYSTEM\TEST.NLM, da der NetWare-Server für den Zugriff auf seine eigene Festplatte keine Laufwerkbuchstaben benutzt.

Sie können im Feld "Befehlszeilenoptionen" beliebige Befehlszeilenoptionen für den zu verwendenden NLM angeben.

Konfigurieren der Alarmaktion "Seite senden"

Mit dieser Alarmaktion wird eine Pager-Nachricht an die von Ihnen angegebene Nummer gesendet. Clients, auf denen diese Alarmaktion konfiguriert wird, müssen ein Modem besitzen. Testen Sie "Seite senden"-Alarmaktionen, um sicherzustellen, dass sie wie gewünscht funktionieren.. Nähere Informationen hierzu finden Sie unter Testen konfigurierter Alarmaktionen weiter unten in diesem Kapitel.

Die Konfiguration von Pager-Alarmaktionen setzt sich wie folgt zusammen:

- Konfigurieren eines Modems für AMS
- Konfigurieren für einen Paging-Dienst
- Eingabe einer Pager-Nachricht

Die drei Abschnitte nach dem nächsten Verfahrensschritt beschreiben die einzelnen Teile dieses Konfigurationsvorgangs genauer.

So konfigurieren Sie die Alarmaktion "Seite senden"

1. Wählen Sie im Dialogfeld "AMS-Alarme konfigurieren" den **Parameter** aus, für den Sie Alarmaktionen konfigurieren möchten.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf die Alarmaktion **Seite senden** und danach auf **Weiter**.
4. Wählen Sie den **Client** aus, auf dem die Aktion ausgeführt werden soll, und klicken Sie dann auf **Weiter**.
5. Wählen Sie einen **Schweregrad für die Alarmaktion**, oder verwenden Sie die Standardeinstellung und klicken Sie dann auf **Weiter**.
6. Geben Sie die **Telefonnummer** ein, die angerufen werden soll. Achten Sie darauf, auch die Zahlen einzugeben, die an Ihrem Standort zum Wählen einer externen Telefonleitung erforderlich sind.
7. Geben Sie die **Pager-Kennung** ein.
8. Geben Sie in das Feld "Kennwort" das **Kennwort** ein, das Sie für den Zugriff auf das Netzwerk des Paging-Dienstes verwenden. Wenn Ihr Paging-Dienst kein Kennwort erfordert, lassen Sie dieses Feld leer.
9. Wählen Sie in der Dropdown-Liste "Dienst" Ihren **Diensttyp** aus. Falls Ihr Paging-Dienst nicht aufgeführt ist, probieren Sie es mit einem der allgemeinen Typen. Weitere Informationen finden Sie unter Konfigurieren für einen Paging-Dienst.
10. Klicken Sie auf **Weiter**.
11. Wenn Sie eine Nachricht für einen alphanumerischen Pager erstellen, geben Sie den **Meldungstext** ein, den Sie im Feld "Meldung" anzeigen möchten, und verschieben Sie die **Parameter**, die Sie verwenden möchten, aus der Liste "Alarmparameter" in das Feld "Meldung". Falls Sie eine Nachricht für einen numerischen Pager erstellen, dürfen Sie in das Feld "Meldung" lediglich Zahlen eingeben.
12. Geben Sie einen **Konfigurationsnamen** ein. Der Konfigurationsname wird im Dialogfeld "AMS-Alarme konfigurieren" neben dieser Aktion angezeigt.
13. Klicken Sie auf **Fertigstellen**.

Konfigurieren eines Modems für AMS

Sie müssen für AMS ein Modem konfigurieren, das zur Kontaktaufnahme mit dem Paging-Dienst verwendet wird. Damit die Alarmaktion "Seite senden" ordnungsgemäß ausgeführt wird, müssen Sie ein Modemkonfigurationsprogramm ausführen und den richtigen COM-Port sowie die korrekten Einstellungen für den Modemtyp wählen.

So konfigurieren Sie ein Modem für AMS

1. Doppelklicken Sie in Windows Explorer auf das Modemkonfigurationsprogramm **MODEMCFG.EXE**. Dieses Dienstprogramm befindet sich auf Windows NT-Clients im Ordner WINNT\SYSTEM32\AMS_ii. Bei Windows 98SE-Clients befindet sich dieses Dienstprogramm im Ordner WINDOWS\SYSTEM\AMS_ii.
2. Wählen Sie in der Dropdown-Liste "COM-Port" den **COM-Port**, an den das Modem angeschlossen ist.
3. Wählen Sie in der Dropdown-Liste "Modemtyp" den richtigen **Modemtyp** aus.
4. Klicken Sie auf **OK**, um diese Einstellungen zu speichern. Das Modem ist nun für die Zusammenarbeit mit dem AMS-Alarmsystem konfiguriert.

Konfigurieren für einen Paging-Dienst

Auf Paging-Dienste kann direkt oder indirekt zugegriffen werden. Die AMS-Alarmaktionen "Seite senden" sind allerdings nur mit direkten Paging-Diensten einsetzbar.

Paging-Methode	**Beschreibung**
Direktes Paging	Damit ist das Wählen der Netzwerkzugriffsnummer des Paging-Dienstanbieters gemeint. Sie greifen zur Angabe der Pager-Kennung auf das Clientnetzwerk des Dienstanbieters zu und das Paging-Dienstnetzwerk sendet die Nachricht dann an den Pager.
Indirektes Paging	Hierzu ist der Anruf bei einem Paging-Dienst und die Weitergabe der Pager-Kennung an die Vermittlung erforderlich. **AMS-Alarme vom Typ "Seite senden" unterstützen kein indirektes Paging.** Weil die Vermittlung des Paging-Dienstes die Daten in das Paging-Netzwerk eingibt, welches die Nachricht an den Pager sendet, kann die AMS-Meldung nicht in das Paging-Dienstnetzwerk gesendet werden. Die indirekte Paging-Methode, die gelegentlich zur direkten Kontaktaufnahme mit dem Netzwerk eingesetzt wird, erfordert einen gebührenpflichtigen Anruf, und der Pager-Dienst bietet über die Vermittlung kostenlose Dienste an.

Sie müssen die Alarmaktion "Seite senden" für Ihren Paging-Dienst konfigurieren. Hierzu ist zumindest die Angabe der Telefonnummer und des Namens des verwendeten Paging-Dienstes erforderlich.

Geben Sie die Telefonnummer des Paging-Dienstes im Dialogfeld für diese Alarmaktion immer in das Feld "Dienstanbieter" ein. Falls Ihr Paging-Dienst nicht in der Dropdown-Liste "Dienst" verzeichnet ist, probieren Sie den Diensttyp "Generisch Signalton" oder "Generisch Alphanumerisch" aus (wählen Sie den Typ, der dem Typ des verwendeten Pager entspricht). Geben Sie in das Feld "Kennwort" das Kennwort ein, das Sie für den Zugriff auf das Netzwerk des Paging-Dienstes verwenden.

Wenn der allgemeine Dienst mit Ihrem Pager nicht funktioniert
Sie müssen die Kommunikationsparameter für die Alarmaktion "Seite senden" konfigurieren. Hierzu gehören Angaben zu Baudrate, Daten- und Stopp-Bits, Parität und Protokoll, die von Ihrem Paging-Dienst verwendet werden. Sie erhalten diese Daten von Ihrem Paging-Dienst. Wenn Ihr Paging-Dienst in der Dropdown-Liste "Dienst" enthalten ist, werden diese Parameter automatisch bei der Auswahl des Dienstes eingestellt.

Wie die Parameter für den Pager-Dienst von Hand konfiguriert werden, wird nachfolgend beschrieben.

So konfigurieren Sie die Pager-Alarmaktion für einen nicht aufgeführten Paging-Dienst

1. Klicken Sie im Pager-Dialogfeld im Feld "Dienst" auf **Neu**.
2. Klicken Sie auf **Eigenschaften**.
3. Geben Sie die für Ihren Paging-Dienst erforderlichen Angaben zu **maximaler Nachrichtenlänge**, **Baudrate**, **Datenbits**, **Stoppbits**, **Parität** und **Protokoll** ein. Sie können diese Daten bei Ihrem Paging-Dienst erfragen.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Weiter**.
6. Wenn Sie eine Nachricht für einen alphanumerischen Pager erstellen, geben Sie den **Meldungstext** ein, den Sie im Feld "Meldung" anzeigen möchten, und verschieben Sie die **Parameter**, die Sie verwenden möchten, aus der Liste "Alarmparameter" in das Feld "Meldung". Falls Sie eine Nachricht für einen numerischen Pager erstellen, dürfen Sie in das Feld "Meldung" lediglich Zahlen eingeben.
7. Geben Sie einen **Konfigurationsnamen** ein. Der Konfigurationsname wird im Dialogfeld "AMS-Alarme konfigurieren" neben dieser Aktion angezeigt.
8. Klicken Sie auf **Fertigstellen**.

Eingabe einer Pager-Nachricht

Die Pager-Alarmaktion unterstützt sowohl alphanumerische als auch rein numerische Pager (so genannte Beeper).

Falls Sie Nachrichten an einen alphanumerischen Pager senden, können diese Nachricht beliebigen von Ihnen eingegebenen Text sowie Informationen über den Alarm enthalten, der die Nachricht erzeugt hat. Diese Nachricht darf die maximale Anzahl von Zeichen, die vom Paging-Dienst unterstützt wird, nicht überschreiten, da sie ansonsten abgeschnitten wird.

Verwenden eines rein numerischen Pagers
Wenn Sie Nachrichten an einen rein numerischen Pager senden, können Sie nur Zahlen verwenden. Definieren Sie ein System aus Servernummern und numerischen Fehlercodes zur Beschreibung der von Ihnen konfigurierten Alarme. Sie können beispielsweise ein System erstellen, in welchem **1** für den Produktionsserver und die Zahl **101** für die Fehlerbedingung "Festplattenkapazität fast erschöpft" steht. Wenn Sie dann die Nachricht **1 101** erhalten, wissen Sie, dass die Festplatte des Produktionsservers fast voll ist.

Konfigurieren der Alarmaktion "SNMP-Trap senden"

SNMP (Simple Network Management Protocol) ist ein nachrichtenbasiertes Protokoll, das auf einem aus Get-, GetNext- und Set-Nachrichten und -Antworten bestehendem Manager/Agentenmodell beruht. SNMP-Traps dienen dazu, Ausnahmenbedingungen zu melden, wie den Ausfall einer Komponente oder das Überschreiten von Schwellenwerten.

AMS kann eine SNMP-Trap-Nachricht erzeugen, wenn ein Alarm ausgelöst wird. Sie können Systeme, die Alarme erzeugen, so konfigureren, dass sie Trap-Nachrichten an eine SNMP-Verwaltungskonsole senden, sofern eine solche vorhanden ist.

SNMP-Ereigniskonsole nicht im Lieferumfang enthalten
Im Lieferumfang von Management Suite ist keine SNMP-Ereigniskonsole zum Anzeigen von SNMP-Traps und Ereignissen enthalten.

So konfigurieren Sie die Alarmaktion "SNMP-Trap senden"

1. Wählen Sie im Dialogfeld "Alarmeinstellungen" den **Parameter** aus, für den Sie Alarmaktionen konfigurieren möchten.
2. Klicken Sie auf **Konfigurieren**.
3. Wählen Sie die **SNMP-Trap**-Alarmaktion aus und klicken Sie danach auf **Weiter**.
4. Wählen Sie den **Client** aus, auf dem die Aktion ausgeführt werden soll, und klicken Sie dann auf **Weiter**.
5. Wählen Sie einen **Schweregrad für die Alarmaktion** aus, oder verwenden Sie die Standardeinstellung und klicken Sie dann auf **Weiter**.
6. Geben Sie einen beliebigen Meldungstext ein, der in der SNMP-Trap-Nachricht angezeigt werden soll, und verschieben Sie die verfügbaren Parameter, die Sie einsetzen möchten, aus der Liste "Alarmparameter" in das Feld "Meldung".
7. Geben Sie einen **Konfigurationsnamen** ein. Dieser Name wird im Dialogfeld "Alarmeinstellungen" neben dieser Aktion angezeigt.
8. Klicken Sie auf **Fertigstellen**.

Sie müssen die Trap-Zieladresse (entweder IP- oder IPX-Adresse) des Clients angeben, an den SNMP-Traps gesendet werden sollen.

So installieren Sie SNMP unter Windows 2000

1. Doppelklicken Sie in der Systemsteuerung von Windows 200 auf **Software**.
2. Klicken Sie im linken Fensterbereich auf **Windows-Komponenten hinzufügen/entfernen**.
3. Wählen Sie **Verwaltungs- und Überwachungsprogramme** aus und klicken Sie auf **Details**.
4. Wählen Sie **SNMP (Simple Network Management Protocol)** aus und klicken Sie auf **OK**.
5. Klicken Sie auf **Weiter**.
6. Windows 2000 installiert daraufhin die SNMP-Komponenten. Beenden Sie die SNMP-Installation.

So konfigurieren Sie Trapziele für Windows 2000

1. Klicken Sie im Systemsteuerungsmodul "Computerverwaltung" auf **Dienste und Anwendungen** und dann auf **Dienste**.
2. Doppelklicken Sie auf **SNMP-Dienst**.
3. Klicken Sie auf die Registerkarte "Traps".
4. Geben Sie **Öffentlich** in das Listenfeld **Communityname** ein und klicken Sie auf **Zur Liste hinzufügen**.
5. Geben Sie unter **Trapziele** die Clients an, an die Traps gesendet werden sollen, und klicken Sie dann auf **Hinzufügen**.
6. Klicken Sie auf **OK**.

So konfigurieren Sie Trapziele für Windows NT 4

1. Doppelklicken Sie in der Systemsteuerung von Windows NT auf das **Netzwerksymbol**.
2. Klicken Sie auf die Registerkarte **Dienste**.
3. Klicken Sie auf **SNMP-Dienst** und dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte "Traps".
5. Wählen Sie in der Dropdown-Liste "Communityname" den Eintrag **Öffentlich** aus. Falls die Liste keinen Eintrag namens "Öffentlich" enthält, tragen Sie ihn ein und klicken dann auf **Hinzufügen**.
6. Nachdem Sie den Communitynamen "Öffentlich" ausgewählt oder eingegeben haben, klicken Sie unter der Liste "Trapziele" auf **Hinzufügen**.
7. Geben Sie die **Adressen** der Clients an, an die Traps gesendet werden sollen, und klicken Sie dann auf **Hinzufügen**.
8. Klicken Sie auf **OK | Schließen**.

So konfigurieren Sie Trapziele für NetWare 5.1-Server

1. Geben Sie auf der NetWare-Serverkonsole Folgendes ein:
   `load install`
2. Klicken Sie auf **Product Options** (Produktoptionen)
3. Klicken Sie auf **Configure Network Protocols** (Netzwerkprotokolle konfigurieren).
4. Klicken Sie auf **Protocols** (Protokolle).
5. Klicken Sie auf **TCP/IP**.
6. Klicken Sie auf **SNMP Manager Table**.
7. Geben Sie die **Adressen** der Clients an, an die Traps gesendet werden sollen, und klicken Sie dann auf **Hinzufügen**.

Arbeiten mit konfigurierten Alarmaktionen

Nachdem Sie Alarmaktionen konfiguriert haben, können Sie sie testen, um sicherzustellen, dass wie sie erwartet funktionieren, Sie können sie löschen und sie in andere Clients exportieren.

Testen konfigurierter Alarmaktionen

Nach der Konfiguration von Alarmaktionen testen Sie diese im Dialogfeld "Alarmeinstellungen".

So testen Sie konfigurierte Alarmaktionen

- Klicken Sie mit der rechten Maustaste auf einen **Alarm** und klicken Sie dann auf **Test**, um alle für diesen Alarm konfigurierten Alarmaktionen zu testen. Klicken Sie mit der rechten Maustaste auf eine bestimmte **Alarmaktion** und klicken Sie dann auf **Testen**, damit die betreffende Alarmaktion ausgeführt wird.

Löschen von Alarmaktionen aus einem Parameter

Sie können eine Alarmaktion aus einem Parameter löschen

So löschen Sie eine Alarmaktion aus einem Parameter

1. Klicken Sie im Dialogfeld "Alarmeinstellungen" mit der rechten Maustaste auf die **Alarmaktion**, die Sie löschen möchten.
2. Klicken Sie auf **Löschen**.

Exportieren von Alarmaktionen in andere Clients

Jeder Client, der AMS-Alarme erzeugt, speichert seine Alarminformationen in einer lokalen AMS-Datenbank. Normalerweise sind die in einer Datenbank gespeicherten Alarme und Aktionen für die AMS-Datenbanken anderer Clients nicht sichtbar. Gelegentlich möchten Sie die Konfigurationen von AMS-Alarmaktionen vielleicht auf mehrere Clients kopieren, damit Sie die erforderlichen Schritte dort nicht erneut ausführen müssen. Die AMS-Exportoption ermöglicht es Ihnen, Alarmaktionen in andere Clients, die AMS-Alarme erzeugen, zu exportieren.

Möglicherweise funktionieren nicht alle Alarmaktionen auf anderen Clients. Wenn Sie beispielsweise eine Alarmaktion vom Typ "Seite senden" in einen Client exportieren, der kein Modem besitzt, dann kann diese Alarmaktion nicht ausgeführt werden.

Sie können eine einzelne Alarmaktion oder sämtliche Alarmaktionen von einem Client in andere Clients exportieren.

So exportieren Sie Alarmaktionen in andere Clients

1. Klicken Sie im Dialogfeld "Alarmeinstellungen" mit der rechten Maustaste auf einen **Alarm** (wenn Sie alle AMS-Alarmaktionen dieses Clients exportieren möchten) oder auf eine bestimmte Alarmaktion (wenn Sie nur die ausgewählte Alarmaktion exportieren möchten).
2. Klicken Sie auf **Exportieren**.
3. Wählen Sie im Dialogfeld "Computer für Empfang der exportierten Aktionen auswählen" die **Computer** aus, an die die von Ihnen ausgewählten Alarmaktionen übertragen werden sollen. Falls der gewünschte Client nicht in der Liste "Verfügbare Computer" verzeichnet ist, obwohl AMS darauf ausgeführt wird, klicken Sie auf **Aktualisieren**, damit die Clients von AMS erneut erfasst werden.
4. Klicken Sie auf **Exportieren**.
5. Überprüfen Sie im Dialogfeld "Exportstatus", ob die Alarmaktionen erfolgreich exportiert wurden.

Anzeigen des Exportstatus

Nachdem die AMS-Alarmaktionen in die von Ihnen ausgewählten Clients exportiert wurden, zeigt AMS die Exportergebnisse im Dialogfeld "Exportstatus" an. In diesem Dialogfeld werden die Alarmaktionen aufgeführt, die nicht erfolgreich exportiert wurden. Der Export von Alarmaktionen kann aus folgenden Gründen fehlschlagen:

- AMS ist auf dem Zielclient nicht installiert oder funktioniert dort nicht richtig. Überprüfen Sie AMS, indem Sie aus dem Dialogfeld "Alarmeinstellungen" heraus eine konfigurierte Alarmaktion auf dem betreffenden Client testen.
- Der Alarm, für den die Aktion konfiguriert wurde, ist auf dem Zielclient nicht verfügbar. Stellen Sie sicher, dass die Anwendung, die auf dem Quellclient den Alarm bei AMS registriert hat, auf dem Zielclient installiert ist.

Anzeigen des AMS-Warnungsprotokolls

Sie können mithilfe des AMS-Warnungsprotokolls der Konsole eine Liste aller AMS-Alarme anzeigen, die von Clients im Netzwerk erzeugt wurden. Das Warnungsprotokoll kann konfiguriert werden, sodass Folgendes angezeigt wird:

- Nur diejenigen Alarme, die die angegebenen Bedingungen erfüllen
- Eine bestimmte Anzahl von Einträgen

Die Liste der Alarme wird im Dialogfeld "Warnungsprotokoll" mit folgenden Informationen zu jedem Alarm angezeigt:

- Alarmname
- Quelle
- Computer
- Datum
- Uhrzeit
- Schweregrad

Zusätzlich zu den Grunddaten, die im Dialogfeld "Warnungsprotokoll" angezeigt werden, sind im Dialogfeld "Alarminformationen" detaillierte Informationen über jeden Alarm verfügbar. Die Daten über das AMS-Warnungsprotokoll werden für alle Client-Arbeitsplatzrechner und Konsolen auf dem Core Server gespeichert.

So zeigen Sie das AMS-Warnungsprotokoll an

- Klicken Sie in der Konsole auf **Ansicht | Warnungsprotokoll**, um das Warnungsprotokoll anzuzeigen.

Filtern der im Warnungsprotokoll angezeigten Liste

Sie können das Warnungsprotokoll so konfigurieren, dass nur diejenigen Alarme angezeigt werden, die den von Ihnen angegebenen Kriterien entsprechen. Mithilfe der folgenden Parameter können Sie filtern, welche Alarme angezeigt werden:

Filter	Beschreibung
Von-/Bis-Ansicht	Legt den Datums- und Uhrzeitbereich der anzuzeigenden Alarme fest.
Computer	Zeigt von einem bestimmten Client ausgegebene Alarme an.
Quelle	Zeigt Alarme an, die von der gleichen Alarmquelle (z. B. dem Fernsteuerungsagenten) auf einem oder mehreren Clients ausgegeben wurden.
Alarm	Zeigt alle Alarme mit dem angegebenen Alarmnamen an.

Schweregrad	Zeigt nur diejenigen Alarme an, die den von Ihnen ausgewählten Schweregrad besitzen. Sie können die folgenden Schweregrade angeben: Monitor, Information, OK, Nicht-kritisch, Kritisch und Nicht-wiederherstellbar.

So geben Sie an, welche Alarme im Warnungsprotokoll angezeigt werden

1. Klicken Sie mit der rechten Maustaste in das Fenster **Warnungsprotokoll** und klicken Sie dann auf "Optionen".
2. Wählen Sie auf der Registerkarte "Filter" die Filter aus, die auf die Liste "Warnungsprotokoll" angewendet werden sollen.
3. Klicken Sie auf **OK**.

So ändern Sie die Anzahl der Einträge, die im Warnungsprotokoll angezeigt werden

1. Klicken Sie mit der rechten Maustaste in das Fenster **Warnungsprotokoll** und klicken Sie dann auf "Optionen".
2. Geben Sie auf der Registerkarte **Einstellungen**, die Anzahl der Einträge an, die im Protokoll gespeichert werden soll.
3. Klicken Sie auf **OK**.

Anzeigen detaillierter Informationen zu Alarmen

Zu jedem Alarm, der im Fenster "Warnungsprotokoll" angezeigt wird, sind detaillierte Informationen verfügbar. Die detaillierten Informationen werden im Dialogfeld "Alarminformationen" angezeigt und umfassen Alarmparameter, deren Werte und den Aktionsstatus eines jeden Alarms.

Das Dialogfeld "Alarminformationen" enthält zudem folgende Informationen:

Aktionsstatus	Beschreibung
Aktionstyp	Art der Aktion, die durch den Alarm erzeugt wird, z. B. Meldungsfeld, Pager, Internet-Mail, Programmausführung oder Broadcast.
Aktionsname	Name, der der betreffenden Aktion zugewiesen wurde
Computer	Name des Clients, auf dem der Alarm ausgegeben werden soll
Status	Alarmstatus, beispielsweise ausstehend, in Bearbeitung, Fehler, erfolgreich abgeschlossen oder fehlgeschlagen.

So zeigen Sie Alarminformationen an

1. Doppelklicken Sie im Fenster "Warnungsprotokoll" auf den **Alarm**, zu dem detaillierte Informationen angezeigt werden sollen.
2. Nachdem Sie die Alarminformationen betrachtet haben, klicken Sie auf **Schließen**.

Bei dem Client, der im Warnungsprotokoll aufgeführt wird, handelt es sich um den Core Server, der die Aktion aufgezeichnet hat. Der Core Server zeichnet alle Ereignisse auf.

So zeigen Sie an, welcher Client einen Alarm ausgegeben hat

- Doppelklicken Sie auf den **Eintrag im Warnungsprotokoll**, zu dem detaillierte Informationen angezeigt werden sollen. Im Fenster "Alarminformationen" werden zusätzliche Alarmangaben angezeigt, darunter auch der Name des Clients, der den Alarm ausgegeben hat.

Löschen von Warnungsprotokolleinträgen

Sie können sowohl einzelne Einträge als auch Gruppen von Einträgen aus dem Warnungsprotokoll löschen.

So löschen Sie einen einzelnen Protokolleintrag

- Wählen Sie den Protokolleintrag aus, den Sie löschen möchten. Klicken Sie dann mit der rechten Maustaste in das Fenster **Warnungsprotokoll** und klicken Sie dann auf **Löschen | Ausgewählte Einträge**.

So löschen Sie mehrere Protokolleinträge

1. Halten Sie die **Strg-Taste** gedrückt, während Sie die zu löschenden Einträge auswählen.
2. Klicken Sie mit der rechten Maustaste in das Fenster **Warnungsprotokoll** und klicken Sie dann auf **Löschen | Ausgewählte Einträge**.

So löschen Sie alle angezeigten Protokolleinträge

1. Filtern Sie das Warnungsprotokoll, sodass nur diejenigen Einträge, die Sie löschen möchten, angezeigt werden.
2. Klicken Sie mit der rechten Maustaste in das Fenster **Warnungsprotokoll** und klicken Sie dann auf **Löschen | Gefilterte Einträge**.

Kopieren des Inhalts des Warnungsprotokolls in die Zwischenablage

Sie können die Einträge des Warnungsprotokolls und deren Parameter in die Zwischenablage kopieren, damit Sie sie zum Drucken oder zur Datenanalyse in eine andere Anwendung einfügen können.

Es werden nur die Parameter kopiert, die im Protokoll sichtbar sind. Um die Anzahl der Einträge zu beschränken, die in die Zwischenablage kopiert werden, beschränken Sie durch die Anwendung von Filtern die Anzahl der im Warnungsprotokoll angezeigten Einträge.

So kopieren Sie den Inhalt des Warnungsprotokolls in die Zwischenablage

1. Passen Sie die **Protokollfilter** so an, dass nur die Einträge, die Sie kopieren möchten, sichtbar bleiben.
2. Klicken Sie mit der rechten Maustaste in das Fenster **Warnungsprotokoll** und klicken Sie dann auf **Kopieren**.

Kapitel 13: Verwenden des Patch Manager-Zusatzprodukts

LANDesk Patch Manager 8 bietet Ihnen eine komplette Patch Management-Lösung — einschließlich automatisierter Aktualisierung von Anfälligkeits-, Bewertungs- und Fehlerbehebungsinformationen — die in das Management Suite 8-Netzwerk integriert werden kann.

Patch Manager 8 Add-on
Patch Manager ist ein separat erworbenes Add-on-Produkt, das Ihr vorhandenes LANDesk Management Suite 8-System optimal ergänzt. Wenn Sie Patch Manager nicht erworben oder installiert haben, befinden sich die in diesem Kapitel beschriebene Benutzeroberfläche und Funktionen nicht auf dem Core Server und stehen Ihnen in der Management Suite-Konsole nicht zur Verfügung. Weitere Informationen zum Erwerb von Patch Manager finden Sie auf der LANDesk-Website.

Weitere Informationen zur Installation und Aktivierung des Patch Manager-Add-On finden Sie unter "Installieren von Add-Ons" im *Installations- und Verteilungshandbuch*.

In diesem Kapitel erfahren Sie mehr über:

- Übersicht über Patch Manager
- Informationen zum Patch Manager-Fenster
- Konfigurieren von Clients für den Patch Manager
- Aktualisieren von Anfälligkeits- und Erkennungsregelinformationen
- Erstellen benutzerdefinierter Anfälligkeits- und Erkennungsregeln
- Anzeigen von Anfälligkeits- und Erkennungsregelinformationen
- Löschen von Anfälligkeits- und Erkennungsregelinformationen
- Scannen von Clients auf Anfälligkeiten
- Anzeigen erkannter Anfälligkeiten
- Herunterladen von Patches
- Reparieren von Anfälligkeiten
- Verwenden von Patch Manager-Berichten

Übersicht über Patch Manager

Patch Manager stellt Ihnen alle Tools zur Verfügung, die Sie für die Einrichtung der Sicherheit auf Patchebene im Netzwerk benötigen. Mit dem Patch Manager können Sie sich wiederholende Prozesse automatisieren, z.B. die Verwaltung aktueller Anfälligkeitsinformationen, die Einschätzung der Anfälligkeiten verschiedener Betriebssysteme und Anwendungen, die auf den verwalteten Geräten ausgeführt werden, das Herunterladen entsprechender ausführbarer Patchdateien, das Reparieren von Anfälligkeiten durch die Verteilung und Installation notwendiger Patches auf Clients und die Überprüfung einer erfolgreichen Patchinstallation.

Sie können zudem eigene benutzerdefinierte Anfälligkeitsdefinitionen erstellen, um verwaltete Geräte auf bestimmte Betriebssystem- und Anwendungsbedingungen hin zu überprüfen, die den Betrieb und die Sicherheit Ihres Systems beeinträchtigen könnten. Benutzerdefinierte (von Ihnen bearbeitete) Anfälligkeiten können entweder nur für die Erkennung oder für die Erkennung und Reparatur entwickelt werden. Weitere Informationen finden Sie unter "Erstellen von benutzedefinierten Anfälligkeits- und Erkennungsregeln" weiter unten in diesem Kapitel.

Patch Manager verwendet die rollenbasierte Administration der Management Suite, um Benutzern Zugriff auf die Patch Manager-Werkzeuge zu ermöglichen Die rollenbasierte Administration ist das Zugriffs- und Sicherheitsmodell der Management Suite, mit dem LANDesk Administratoren den Zugriff auf Tools und Geräte einschränken können. Jedem Management Suite-Benutzer werden bestimmte Rechte und Bereiche zugewiesen, die festlegen, mit welchen Funktionen dieser Benutzer arbeiten und welche Geräte er verwalten kann. Weitere Informationen finden Sie unter "Verwenden der rollenbasierten Administration" in Kapitel 1. Ein LANDesk Administrator weist diese Rechte mithilfe des Benutzerwerkzeugs in der Hauptkonsole der Management Suite anderen Benutzern zu. Patch Manager erweitert die rollenbasierte Administration um eine neue Rolle und das damit verbundene Recht. Dieses Recht heißt ganz einfach "Patch Manager" und wird im Dialogfeld "Benutzereigenschaften" angezeigt. Um Patch Manager anzeigen und verwenden zu können, muss einem Management Suite-Benutzer wie unten beschrieben das erforderliche Patch Manager-Recht erteilt werden.

Der Patch Manager unterstützt die meisten LANDesk Management Suite-Standard-Clientplattformen. Dadurch können Sie auf verwalteten Clients mit den folgenden Betriebssystemen nach Anfälligkeiten suchen und Sicherheitspatches verteilen:

Unterstützte Plattformen

- Windows 95B/98 SE
- Windows NT (4.0 SP6a und höher)
- Windows 2000 SP4/2003/XP SP1
- Sun Solaris
- Mac OS X 10.2.x und 10.3.x

Weitere Informationen zur Einrichtung der verwalteten Clients im Netzwerk für das Scannen auf Anfälligkeiten und die Patchverteilung finden Sie unter "Konfigurieren von Clients für den Patch Manager" weiter unten in diesem Kapitel.

Mit den Patch Manager-Funktionen können Sie folgende Funktionen ausführen:

- Verwalten aktualisierter Anfälligkeits- und Patchinformationen (über den LANDesk Patch Manager-Dienst, der Daten aus mehreren Anfälligkeitsdatenquellen der IT-Branche (Hersteller, Händler etc.) konsolidiert).
- Bereitstellen von Patchsicherheit für internationale Versionen der Betriebssysteme im Netzwerk, einschließlich Unterstützung der folgenden Sprachen: Englisch, Japanisch, Französisch, Deutsch, Italienisch, Spanisch und Schwedisch.
- Erstellen eigener benutzerdefinierter Anfälligkeiten zur Erkennung und Reparatur von Anfälligkeiten.
- Organisieren und Gruppieren der Anfälligkeiten zur Ausführung benutzerdefinierter Anfälligkeitsbewertungen und -reparaturen.
- Anfälligkeitseinschätzung auf mehreren unterstützten Clientplattformen einschließlich Windows und Sun Solaris.
- Anzeigen von Anfälligkeits- und Erkennungsregeldetails für jedes verwaltete Gerät über die Management Suite-Konsole.
- Planen automatischer Patchverwaltungsaufgaben, einschließlich Anfälligkeitsaktualisierungen, Gerätescans und Patchdownloads.
- Reparatur als geplanter Task, Richtlinie oder automatisch über die Funktion "Automatisches Korrigieren".
- Herunterladen und Verteilen von Patches, die untersucht und überprüft wurden.
- Verfolgen des Status von Patchverteilungen und -Installation auf Zielgeräten.
- Verwenden der Funktionen "Targeted Multicast", "Peerdownload" und "Checkpunkt-Neustart" der Management Suite für eine schnelle und effiziente Patchverteilung.
- Generieren und Anzeigen erkannter Anfälligkeits- und Reparaturstatusinformationen mit einer Reihe von patchverwaltungsspezifischen Berichten.

In den folgenden Schritten werden die Anfälligkeitseinschätzungen und die Reparaturprozesse beschrieben, die bei der Implementierung der Patchverwaltung im Management Suite-Netzwerk enthalten sind. (Diese Vorgehensweisen werden in den entsprechenden Abschnitten unten näher erläutert.)

1. Sammeln aktualisierter Anfälligkeitsinformationen aus den Datenquellen der IT-Branche. Erstellen eigener benutzerdefinierter Anfälligkeiten.
2. Organisieren und Anzeigen von Anfälligkeitsinformationen.
3. Konfigurieren der Clients für Anfälligkeitsscan und Patchverteilung.
4. Scannen der Geräte im Netzwerk auf Anfälligkeiten.
5. Anzeigen der Ergebnisse für die gescannten Geräte.
6. Herunterladen von Sicherheitspatches für erkannte Anfälligkeiten.
7. Reparieren von Anfälligkeiten durch die Patchverteilung an betroffene Clients.
8. Anzeigen des Patchverteilungsstatus.

Informationen zum Patch Manager-Fenster

Das Patch Manager-Fenster wird wie alle anderen Management Suite-Werkzeugfenster entweder über das Menü "Extras" oder die Toolbox geöffnet. Es kann mit anderen offenen Werkzeugfenstern verankert oder unverankert sein oder über Registerkarten verfügen (siehe "Verankerbare Fenster" in Kapitel 1). Beachten Sie, dass ein Management Suite-Benutzer bei der neuen Funktion für rollenbasierten Administrationszugriff und Sicherheit in Management Suite 8 über LANDesk-Administratorrechte (d.h. volle Rechte) oder über Patch Manager-Rechte verfügen muss, damit er auf das Patch Manager-Werkzeug zugreifen kann. Weitere Informationen zu Benutzerrechten und Bereich finden Sie unter "Verwenden der rollenbasierten Administration" in Kapitel 1.

Das Patch Manager-Fenster enthält eine Symbolleiste und zwei Fensterausschnitte. Der linke Fensterausschnitt zeigt eine hierarchische Strukturansicht der Anfälligkeits- und Erkennungsregelgruppen. Sie können alle Strukturobjekte nach Bedarf erweitern oder reduzieren. Der rechte Fensterausschnitt zeigt eine detaillierte Liste der Anfälligkeiten oder Erkennungsregeln der ausgewählten Gruppen, abhängig von der Art der ausgewählten Gruppe.

Schaltflächen der Symbolleiste

- **Anfälligkeitsinformationen aktualisieren:** Öffnet das Dialogfeld "Anfälligkeitseinstellungen aktualisieren". Hier können Sie die Plattformen und Sprachen angeben, deren Anfälligkeitsinformationen Sie aktualisieren möchten. Sie können außerdem festlegen, ob die Anfälligkeiten in der Gruppe "Aktivierte Anfälligkeiten" abgelegt und ob gleichzeitig verknüpfte Patches heruntergeladen werden sollen, und Sie geben den Speicherort für heruntergeladene Patches und die Proxy-Server-Einstellungen an.
- **Periodische Aktualisierung planen:** Erstellt einen Task für die Aktualisierung der Anfälligkeitsinformationen, der im Fenster "Geplante Tasks" angezeigt wird. In diesem Fenster können Sie die Planungsoptionen konfigurieren.
- **Anfälligkeitsscan planen:** Erstellt einen Task für den Anfälligkeitsscan, der im Fenster "Geplante Tasks" angezeigt wird. In diesem Fenster können Sie Zielgeräte hinzufügen und den Task planen.
- **Aktualisieren:** Aktualisiert den Inhalt der ausgewählten Gruppe.
- **Neue Anfälligkeit erstellen:** Öffnet ein neues Dialogfeld "Anfälligkeitseigenschaften" mit editierbaren Feldern, in denen Sie den Anfälligkeitsdefinitionstyp (nur Erkennung oder Erkennung und Reparatur) bestimmen können, Anfälligkeitsinformationen eingeben, Erkennungsregeln erstellen und die entsprechende Patchdatei identifizieren können.
- **Benutzerdefinierte Anfälligkeiten importieren:** Hiermit können Sie eine XML-Datei importieren, die eine Anfälligkeitsdefinition beinhaltet.
- **Benutzerdefinierte Anfälligkeiten exportieren:** Hiermit können Sie eine Anfälligkeitsdefinition als XML-Datei exportieren.
- **Benutzerdefinierte Anfälligkeiten löschen:** Entfernt die ausgewählten benutzerdefinierten Anfälligkeiten aus der Core-Datenbank.

- **Nicht verwendete Anfälligkeiten entfernen:** Öffnet das Dialogfeld "Nicht verwendete Anfälligkeiten entfernen ". Hier können Sie die Plattformen und Sprachen angeben, deren Anfälligkeitsinformationen Sie aus der Core-Datenbank entfernen möchten.
- **Hilfe:** Öffnet die Online-Hilfe.

Der linke Fensterausschnitt des Patch Manager-Fensters zeigt die folgenden Elemente:

Hauptansicht

Die Hauptansicht ist der Stamm des Patch Manager-Baums. Sie enthält die Anfälligkeits- und Erkennungsregelgruppen und kann erweitert und reduziert werden.

Identifizieren benutzerdefinierter Anfälligkeiten
Sie erkennen benutzerdefinierte Anfälligkeiten immer an dem kleinen Personensymbol, ganz gleich, ob sich die Anfälligkeiten in der Gruppe "Aktiviert", "Deaktiviert" oder "Nicht zugewiesen" befinden.

Anfälligkeiten

Die Anfälligkeitsgruppe enthält die folgenden Untergruppen:

- **Aktivierte Anfälligkeiten:** Führt alle Anfälligkeiten auf, nach denen gesucht wird, wenn der Anfälligkeitsscanner auf verwalteten Geräten ausgeführt wird. Das heißt, wenn eine Anfälligkeit in diese Gruppe einbezogen wird, ist sie Teil des nächsten Scanvorgangs. Andernfalls ist sie es nicht.

  "Aktiviert" kann als einer von drei Anfälligkeitszuständen betrachtet werden. Die anderen beiden sind "Deaktiviert" und "Nicht zugewiesen". Eine Anfälligkeit kann sich immer nur in jeweils einer dieser drei Gruppen befinden. Eine Anfälligkeit ist entweder "Aktiviert", "Deaktiviert" oder "Nicht zugewiesen". Für jeden Zustand gibt es ein eindeutiges Symbol (ein Fragezeichen (?) für "Nicht zugewiesen, ein rotes X für "Deaktiviert" und das reguläre Anfälligkeitssymbol für "Aktiviert"). Beim Verschieben einer Anfälligkeit von einer Gruppe in ein andere ändert sich automatisch ihr Zustand.

  Sie können eine oder mehrere Anfälligkeiten mit Ziehen-und-Ablegen aus einer Gruppe (mit Ausnahme der Gruppe "Erkannte Anfälligkeiten") in die andere verschieben. Indem Sie Anfälligkeiten in die Gruppe "Aktivierte Anfälligkeiten" verschieben, können Sie Art und Größe des nächsten Anfälligkeitsscans auf Zielclients kontrollieren.

  Neue Anfälligkeiten können während einer Aktualisierung automatisch zur Gruppe "Aktivierte Anfälligkeiten" hinzugefügt werden, indem Sie die Option **Neue Anfälligkeiten in Gruppe "Aktiviert" verschieben** im Dialogfeld **Anfälligkeitseinstellungen aktualisieren** aktivieren.

Vorsicht beim Verschieben von Anfälligkeiten aus der Gruppe "Aktivierte Anfälligkeiten"
Wenn Sie Anfälligkeiten aus der Gruppe "Aktiviert" in die Gruppe "Deaktiviert" verschieben, werden die aktuellen Informationen darüber, auf welchen gescannten Clients die Anfälligkeiten erkannt wurden, aus der Core-Datenbank entfernt. Sie stehen somit nicht mehr im Dialogfeld "Eigenschaften" der Anfälligkeiten bzw. im Dialogfeld "Anfälligkeitsinformationen" des Clients zur Verfügung. Um diese Anfälligkeitsbewertungsdaten wiederherzustellen, müssten Sie die Anfälligkeiten wieder in die Gruppe "Aktiviert" schieben und einen neuen Anfälligkeitsscan durchführen.

- **Deaktivierte Anfälligkeiten:** Führt die Anfälligkeiten auf, nach denen nicht gesucht wird, wenn der Anfälligkeitsscanner das nächste Mal auf Geräten ausgeführt wird. Wie oben bereits erwähnt, kann eine in dieser Gruppe enthaltene Anfälligkeit nicht in der Gruppe "Aktiviert" oder "Nicht zugewiesen" enthalten sein. Sie können Anfälligkeiten in diese Gruppe verschieben, um sie vorübergehend aus dem Anfälligkeitsscan auszuschließen.
- **Erkannte Anfälligkeiten:** Zeigt alle Anfälligkeiten für alle Zielgeräte in diesem Scanauftrag, die beim letzten Anfälligkeitsscan erkannt wurden. Der Inhalt dieser Gruppe wird immer vom letzten Anfälligkeitsscan im Netzwerk bestimmt, d.h. davon, ob ein Gerät oder mehrere gescannt wurden.

  Die Liste "Erkannte Anfälligkeiten" setzt sich aus allen beim letzten Scan gefundenen erkannten Anfälligkeiten zusammen. Die Spalten "Gescannt" und "Erkannt" geben an, wie viele Geräte gescannt wurden und auf wie vielen davon die Anfälligkeit erkannt wurde. Wenn Sie sehen möchten, auf welchen Geräten eine Anfälligkeit erkannt wurde, klicken Sie mit der rechten Maustaste auf die Anfälligkeit und wählen **Betroffene Computer**.

  Beachten Sie, dass Sie auch gerätespezifische Anfälligkeitsinformationen anzeigen können, indem Sie mit der rechten Maustaste auf ein Gerät in der Netzwerkansicht klicken und anschließend **Anfälligkeitsinformationen** wählen.

  Sie können nur Anfälligkeiten aus der Gruppe "Erkannte Anfälligkeiten" in die Gruppe "Nicht zugewiesen" oder "Deaktiviert" verschieben.
- **Nicht zugewiesene Anfälligkeiten:** Führt alle Anfälligkeiten auf, die weder zur Gruppe "Aktiviert" noch zur Gruppe "Deaktiviert" gehören. Die Gruppe "Nicht zugewiesene Anfälligkeiten" ist im Wesentlichen ein Wartebereich für gesammelte Anfälligkeiten, bis Sie entscheiden, ob danach gescannt werden soll oder nicht.

  Gesammelte Anfälligkeiten werden während einer Aktualisierung standardmäßig zur Gruppe "Nicht zugewiesene Anfälligkeiten" hinzugefügt.

  Sie können Anfälligkeiten aus der Gruppe "Nicht zugewiesene Anfälligkeiten" in die Gruppe "Aktiviert" oder "Deaktiviert" verschieben (verschieben Sie eine oder mehrere mit Ziehen-und-Ablegen).

- **Benutzerdefinierte Anfälligkeiten:** Zeigt alle benutzerdefinierten Anfälligkeiten, die Sie erstellt haben. Diese Gruppe zeigt immer eine einfache Liste (ohne Untergruppe) mit allen Ihren benutzerdefinierten Anfälligkeiten an, selbst wenn Sie eine Anfälligkeit in die Gruppe "Nicht zugewiesen", "Aktiviert" oder "Deaktiviert" verschoben haben (die Gruppe oder der Zustand der benutzerdefinierten Anfälligkeit wird durch ein sich dynamisch veränderndes Symbol signalisiert).

  Weitere Informationen zum Erstellen, Importieren, Exportieren und Löschen benutzerdefinierter Anfälligkeiten finden Sie unter "Erstellen benutzerdefinierter Anfälligkeiten" weiter unten in diesem Kapitel.

- **Nach Plattform:** Führt alle Anfälligkeiten nach Plattformuntergruppen sortiert auf. Diese Untergruppen helfen Ihnen dabei, Anfälligkeiten nach Plattformkategorie zu unterscheiden.

  Sie können diese Plattformuntergruppen dazu verwenden, Anfälligkeiten in die Gruppe "Aktivierte Anfälligkeiten" für betriebssystemspezifische Scanvorgänge zu kopieren oder um Anfälligkeiten in eine benutzerdefinierte Gruppe (siehe unten) zu kopieren, um eine Gruppe von Anfälligkeiten auf einmal zu reparieren.

  Anfälligkeiten können aus einer Plattformgruppe in die Gruppe "Aktiviert", "Deaktiviert" oder "Nicht zugewiesen" oder in eine der benutzerdefinierten Gruppen kopiert werden (mit Ziehen-und-Ablegen eine oder mehrere kopieren). Anfälligkeiten können gleichzeitig in Plattform-, Produkt- und mehrfachen Kundengruppen vorkommen. (Den Status einer Anfälligkeit erkennen Sie an ihrem Symbol.)

Hinweis: Es kann hilfreich sein, sich die Gruppen "Aktiviert", "Deaktiviert" und "Nicht zugewiesen" als Container für Anfälligkeiten vorzustellen, die sich gegenseitig ausschließen, da eine Anfälligkeit sich jeweils nur in einer der drei Gruppen/Stati befinden kann. Die Gruppe "Erkannte Anfälligkeiten" ist der Container für Scanergebnisse, während Sie mit den Plattform-, Produkt- und benutzerdefinierten Gruppen Anfälligkeiten nach unterschiedlichen Kategorien anzeigen und organisieren können, wenn Sie Scan- und Reparaturtasks konfigurieren.

- **Nach Produkt:** Führt alle Anfälligkeiten nach Produktuntergruppen sortiert auf. Diese Untergruppen helfen Ihnen dabei, Anfälligkeiten nach Produktkategorie zu unterscheiden.

  Sie können diese Produktuntergruppen dazu verwenden, Anfälligkeiten in die Gruppe "Aktivierte Anfälligkeiten" für produktspezifische Scanvorgänge zu kopieren oder um Anfälligkeiten in eine benutzerdefinierte Gruppe (siehe unten) zu kopieren, um eine Gruppe von Produkten auf einmal zu reparieren.

  Anfälligkeiten können aus einer Produktgruppe in die Gruppe "Aktiviert", "Deaktiviert" oder "Nicht zugewiesen" oder in eine der benutzerdefinierten Gruppen kopiert werden (mit Ziehen-und-Ablegen eine oder mehrere kopieren). Anfälligkeiten können gleichzeitig in Plattform-, Produkt- und mehrfachen Kundengruppen vorkommen. (Den Status einer Anfälligkeit erkennen Sie an ihrem Symbol.)

- **Benutzerdefinierte Gruppen:** Führt von Ihnen erstellte Untergruppen und ihre Anfälligkeiten auf. Mithilfe von benutzerdefinierten Gruppen können Sie Anfälligkeiten nach Ihren eigenen Wünschen organisieren. Verwenden Sie den Inhalt einer Gruppe, um mehrere Anfälligkeiten für Scanvorgänge in die Gruppe "Aktivierte Anfälligkeiten" zu kopieren oder um einen Reparaturauftrag für mehrere Anfälligkeiten gleichzeitig zu erstellen.

  Zum Erstellen einer benutzerdefinierten Gruppe klicken Sie mit der rechten Maustaste auf **Benutzerdefinierte Gruppen** (oder eine Untergruppe) und anschließend auf **Neue Gruppe**.

  Um Anfälligkeiten zu einer benutzerdefinierten Gruppe hinzuzufügen, verschieben Sie diese mit Ziehen-und-Ablegen aus anderen Anfälligkeitsgruppen. Sie können auch mit der rechten Maustaste auf eine benutzerdefinierte Gruppe und anschließend auf **Anfälligkeit hinzufügen** klicken.

Patches

Hinweis: Erkennungsregeln definieren das jeweilige Betriebssystem, die Anwendung, die Datei oder die Registrierungsbedingungen, nach der eine Anfälligkeitsdefinition sucht, um eine Anfälligkeit auf einem gescannten Client ausfindig zu machen.

Die Gruppe "Erkennungsregeln" enthält die folgenden Untergruppen:

- **Aktivierte Erkennungsregeln:** Führt alle Erkennungsregeln auf, die für das Scannen auf Geräten aktiviert sind.

  Erkennungsregeln, die mit Anfälligkeiten verknüpft sind, werden während einer Aktualisierung standardmäßig zur Gruppe "Aktivierte Erkennungsregeln" hinzugefügt. Erkennungsregeln, die mit einer benutzerdefinierten Anfälligkeit verknüpft sind, werden während der Erstellung der benutzerdefinierten Anfälligkeit ebenfalls zur Gruppe "Aktivierte Erkennungsregeln" hinzugefügt.

  Beachten Sie, dass Erkennungsregeln nicht nur aktiviert sein müssen, sondern dass die jeweilige ausführbare Patchdatei an einen lokalen Speicherort für Patches in Ihrem Netzwerk heruntergeladen werden muss (i.d.R. auf den Core Server), bevor eine Reparatur stattfinden kann. Das Attribut "Heruntergeladen" (eine der Detailspalten) gibt an, ob das mit dieser Regel assozierte Patch heruntergeladen wurde.
- **Deaktivierte Erkennungsregeln:** Führt alle Erkennungsregeln auf, die für das Scannen auf Geräten deaktiviert sind. Einige Anfälligkeiten sind mit mehreren Regeln verknüpft. Indem Sie eine Regel deaktivieren, können Sie sicherstellen, dass nicht danach gescannt wird.
- **Nach Plattform:** Führt alle Erkennungsregeln der gesammelten Anfälligkeiten nach Plattformuntergruppen sortiert auf. Diese Untergruppen helfen Ihnen dabei, Erkennungsregeln nach Plattformkategorie zu unterscheiden.

  Mithilfe dieser Plattformuntergruppen können Sie Gruppenvorgänge ausführen, wie beispielsweise das Aktivieren/Deaktivieren plattformspezifischer Erkennungsregeln oder Herunterladen mehrerer verknüpfter Patches in einem Arbeitsgang.

- **Nach Produkt:** Führt alle Erkennungsregeln der gesammelten Anfälligkeiten nach Produktuntergruppen sortiert auf. Diese Untergruppen helfen Ihnen dabei, Erkennungsregeln nach Produktkategorie zu unterscheiden.

  Sie können diese Produktuntergruppen verwenden, um Gruppenvorgänge auszuführen.

Der rechte Fensterbereich des Patch Manager-Fensters zeigt wie im Folgenden beschrieben detaillierte Informationen zu Anfälligkeiten und Erkennungsregel-Elementen, aufgelistet in sortierbaren Spalten.

Anfälligkeitsdetails

- **Kennung:** Gibt den eindeutigen, vom Anbieter definierten alphanumerischen Code der Anfälligkeit an.
- **Schweregrad:** Gibt den Schweregrad der Anfälligkeit an. Mögliche Schweregrade sind folgende: Service Pack, Kritisch, Hoch, Mittel, Niedrig, Nicht anwendbar und Unbekannt.
- **Titel:** Beschreibt die Art oder das Ziel der Anfälligkeit in einem kurzen Text.
- **Sprache:** Gibt die Sprache des Betriebssystems oder der Anwendung an, das/die von der Anfälligkeit betroffen ist.
- **Veröffentlichungsdatum:** Gibt das Datum an, an dem die Anfälligkeit vom Anbieter veröffentlicht wurde.
- **Unbeaufsichtigte Installation:** Gibt mit Ja oder Nein an, ob das mit der Anfälligkeit verknüpfte Patch bzw. die verknüpften Patches unbeaufsichtigt (ohne Benutzereingriff) installiert wird/werden. Für einige Anfälligkeiten kann mehr als ein Patch gelten. Wenn einige der Patches einer Anfälligkeit nicht unbeaufsichtigt installiert werden, heißt das entsprechende Attribut Nein. Um zu sehen, wie die einzelnen Patches installiert werden, klicken Sie mit der rechten Maustaste auf die Anfälligkeit und klicken Sie dann auf **Eigenschaften | Patches**.
- **Reparierbar:**Gibt an, ob die Anfälligkeit durch Verteilung und Installation einer Patchdatei repariert werden kann. Zu den möglichen Werten gehören: "Ja", "Nein", "Einige" (für eine Anfälligkeit, die mehrere Erkennungsregeln einschließt, und wenn nicht alle erkannten Anfälligkeiten repariert werden können) und "Keine Regeln" (für eine benutzerdefinierte Anfälligkeit, die keine Erkennungsregeln beinhaltet).
- **Erkannt:** Zeigt die Zahl der gescannten Geräte an, auf denen die Anfälligkeit erkannt wurde.
- **Gescannt:** Zeigt die Zahl der auf die Anfälligkeit gescannten Geräte an.
- **Automatisches Korrigieren:** Gibt an, ob das automatische Korrigieren für die Anfälligkeit aktiviert oder deaktiviert ist.

Klicken Sie mit der rechten Maustaste auf eine Anfälligkeit, um mit der Option "Eigenschaften" weitere Details anzuzeigen. Mit dem Kontextmenü können Sie zudem betroffene Computer anzeigen, das automatische Korrigieren aktivieren/deaktivieren, Scaninformationen und Reparaturstatus löschen und einen Reparaturauftrag erstellen.

Erkennungsregeldetails

- **Regel:** Zeigt den Namen der Erkennungsregel an (kann der Dateiname der ausführbaren Patchdatei sein).
- **Anfälligkeitskennung** Zeigt die Kennung der Anfälligkeit an, mit der die Regel verknüpft ist.
- **Heruntergeladen:** Gibt an, ob die mit der Regel verknüpfte ausführbare Patchdatei in den lokalen Ablageort heruntergeladen wurde. Der Ablageort wird auf der Registerkarte "Patches" des Dialogfelds "Anfälligkeitseinstellungen aktualisieren" konfiguriert.
- **Unbeaufsichtigte Installation:** Gibt mit "Ja" oder "Nein" an, ob das mit der Regel verknüpfte Patch unbeaufsichtigt (ohne Benutzereingriff) auf Clients installiert wird. Zu einer benutzerdefinierten Anfälligkeit gehörende Regeln werden in dieser Spalte als "Benutzerdefiniert" ausgewiesen.

Klicken Sie mit der rechten Maustaste auf eine Anfälligkeit, um mit der Option **Eigenschaften** weitere Details anzuzeigen. Über das Kontextmenü können Sie die Regel aktivieren/deaktivieren und das verknüpfte Patch herunterladen.

Konfigurieren von Clients für den Patch Manager

Bevor verwaltete Clients auf Anfälligkeiten gescannt werden und Patchverteilungen erhalten können, muss auf ihnen der neue Anfälligkeitsscanner-Agent installiert sein.

Hinweis: Auf Windows 9x-Clients ist WinSock2 für die Ausführung des Anfälligkeitsscanner-Agents erforderlich.

Der Patch Manager erfordert außerdem, dass die folgenden Management Suite-Agenten auf den Clients installiert sind:

- Common Base Agent (CBA)
- Bandbreitenerkennungsagent
- Local Scheduler-Agent
- Targeted Multicasting-Agent
- Enhanced Software Distribution-Agent

Application Policy Management-Agent
Wenn Sie richtlinienbasierte Reparaturen durchführen möchten, muss auf den Clients auch der Application Policy Management (APM)-Agent installiert sein.

Bei vorhandenen Clients müssen Sie vermutlich nur den neuen Anfälligkeitsscanner-Agenten installierten, da die anderen Agenten auf den Clients schon installiert sind.

Der einfachste Weg, den Anfälligkeitsscanner-Agenten auf mehrere Windows-Clients zu verteilen, besteht darin, eine neue Clientkonfiguration mit dem Client-Setup-Assistenten zu erstellen. Anschließend planen Sie die Konfiguration für die gewünschten Ziel-Clients mit dem Tool "Geplante Tasks".

So erstellen Sie eine Clientkonfiguration für die Installation des Anfälligkeitsscanner-Agenten

1. Klicken Sie in der Konsole auf **Extras | Clientsetup**.
2. Klicken Sie doppelt auf das Symbol **Neue Konfiguration hinzufügen**, um diese zu erstellen. Wenn Sie lediglich den Anfälligkeitsscanner-Agenten auf bereits konfigurierten Clients hinzufügen, klicken Sie doppelt auf die für die Clientkonfiguration verwendete Konfiguration, um dieselben Einstellungen beizubehalten.
3. Geben Sie einen eindeutigen Namen ein, wenn Sie eine neue Clientkonfiguration erstellen.
4. Wählen Sie auf der Seite "Komponenten installieren" des Client-Setup-Assistenten die Komponente **Anfälligkeitsscanner** aus. Wenn Sie "Anfälligkeitsscanner" auswählen, werden die oben genannten anderen erforderlichen Agenten automatisch ausgewählt. Beachten Sie, dass Sie alle zu installierenden Komponenten auswählen sollten, wenn Sie neue Clients zum ersten Mal konfigurieren.
5. Gehen Sie die verschiedenen Seiten durch, indem Sie auf **Weiter** klicken, und nehmen Sie die notwendigen Änderungen darin vor. Wenn Sie lediglich den Anfälligkeitsscanner-Agenten mit dieser Clientkonfiguration installieren, müssen Sie keine Änderungen an den aktuellen Einstellungen vornehmen.

6. Wenn Sie diese Konfiguration als Standard einrichten möchten (die Konfiguration, die LDLOGON\IPSETUP.BAT installiert), klicken Sie auf **Als Standardkonfiguration festlegen**.
7. Klicken Sie auf **Fertigstellen**, um den Assistenten zu beenden.
8. Klicken Sie mit der rechten Maustaste auf die Konfiguration und anschließend auf **Planen**, um die Konfiguration im Fenster "Geplante Tasks" hinzuzufügen. In diesem Fenster können Sie Ziel-Clients hinzufügen und die Planungsoptionen festlegen.

Weitere Informationen zur Clientkonfiguration
Das Kapitel Clientkonfiguration enthält detaillierte Informationen zur Konfiguration von Clients mit dem Client-Setup-Assistenten und zur Planung von Tasks.

Wenn Sie einen Client für die Unterstützung der Patchverwaltung konfigurieren, werden die benötigten Dateien für das Anfälligkeitsscannen und die Reparatur (d.h. Patchverteilung und -installation) auf dem Ziel-Client installiert. Es wird außerdem ein Programmsymbol für den Anfälligkeitsscanner in der Programmgruppe LANDesk Management des Clients hinzugefügt.

Der Anfälligkeitsscanner wird während des ersten Client-Konfigurationsprozesses automatisch ausgeführt. Bevor Sie Clients konfigurieren, sollten Sie deshalb sicherstellen, dass die Gruppe "Aktivierte Anfälligkeiten" nur die Anfälligkeiten enthält, nach denen gescannt werden soll. Wenn Sie keinen Scan auf Anfälligkeiten wünschen, muss die Gruppe "Aktivierte Anfälligkeiten" leer sein.

Nach der Clientkonfiguration können Sie den Anfälligkeitsscanner direkt auf dem Client mit dem Anfälligkeitsscanner-Programm ausführen. Hierfür müssen Sie den Task "Nach Anfälligkeiten suchen" über die Patch Manager-Symbolleiste erstellen oder das vordefinierte Skript VulnerabilityScan ausführen. Weitere Informationen finden Sie unter "Scannen von Clients auf Anfälligkeiten" weiter unten in diesem Kapitel.

Entfernen des Anfälligkeitsscanners von Clients

Wenn Sie den Anfälligkeitsscanner-Agenten von einem Client entfernen müssen, können Sie ein dafür entwickeltes vordefiniertes Skript verwenden.

So entfernen Sie den Anfälligkeitsscanner

1. Klicken Sie auf **Extras | Geplante Tasks**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Skript planen**.
3. Wählen Sie das Skript **RemoveVulnerabilityScanner**, und klicken Sie auf **OK**.
4. Fügen Sie die gewünschten Ziel-Clients hinzu, und planen Sie den Task.

Sie können auch über das Tool "Skripte verwalten" auf dasselbe Skript zugreifen.

Wenn Sie dieses Skript ausführen, werden die Anfälligkeitsscannerdateien von der Festplatte des Clients entfernt, und das Programmsymbol für den Anfälligkeitsscanner wird aus dem Programmordner LANDesk Management entfernt.

Konfigurieren von UNIX-Clients

LANDesk Management Suite 8 bietet für einige Versionen von Linux und UNIX nur beschränkte Funktionsunterstützung (siehe "Verteilung auf Macintosh-, Linux- und UNIX-Clients" im *Installations- und Verteilungshandbuch*). Der Patch Manager fügt für einige dieser Clients Unterstützung für Anfälligkeitseinschätzung und Reparatur hinzu.

Unterstützte UNIX-Distributionen:

- Sun Sparc (Solaris 8)

Installieren des UNIX-Anfälligkeitsscanner-Agenten

Wie bei den anderen Linux/UNIX-Agenten (z.B. dem Inventarscanner-Agenten) müssen Sie den Anfälligkeitsscanner-Agenten manuell auf den Clients installieren.

Wenn der Patch Manager installiert ist, werden die Anfälligkeitsscanner-Agentendateien in einer einzigen TAR-Datei auf den Core Server kopiert, und zwar in das jeweilige Verzeichnis unter \Programme\LANDesk\ManagementSuite\LDLogon\unix\, das Ihrer UNIX-Distribution entspricht. Derzeit unterstützt Patch Manager Sun Solaris-Clients, somit ist das einzige UNIX-Verzeichnis:

- **solsparc:** Sun Sparc Solaris 8-Verzeichnis

So installieren Sie den Anfälligkeitsscanner auf Sun Solaris-Clients

1. Stellen Sie sicher, dass diese beiden Bibliotheksdateien bereits installiert sind: **libexpat.so** und **libstdc++.so**. Diese beiden Dateien sind erforderlich, damit der Anfälligkeitsscanner auf Solaris-Clients ausgeführt werden kann.
2. Kopieren Sie die Agenten-TAR-Datei (**vulscan-8.0-0.x-solaris.tar.gz**) vom Core Server.
3. Entzippen Sie das TAR-Archiv. Es enthält die Inventaragentendateien (die eventuell bereits auf Ihren Clients installiert sind) und zwei neue Anfälligkeitsagentendateien: die ausführbare Datei **vulscan** und die Konfigurationsdatei **vulscan.conf**.
4. Kopieren Sie **vulscan.conf** nach /etc. Erteilen Sie Lese-/Schreibrechte für Benutzer. Weisen Sie den Dateien mit dem UNIX-Befehl **chmod** Zugriffsberechtigungen zu.
5. Kopieren Sie **vulscan** in ein Verzeichnis, auf das die Personen, die diese Anwendung ausführen werden, Zugriff haben. Beispiel: /usr/local/landesk/PatchManager. Falls erforderlich, machen Sie vulscan mithilfe des Befehls **chmod** ausführbar.

Hinweis: Wenn Sie den Solaris-Client noch nicht mit dem Inventarscanner-Agenten konfiguriert haben, können Sie zu diesem Zeitpunkt auch die Inventaragentendateien verteilen. Weitere Informationen finden Sie in der README-Datei im oben genannten TAR-Archiv.

Konfigurieren von Mac OS X-Clients

Sie können auf Mac OS X-Clients nur auf Anfälligkeiten scannen. Die Reparatur muss manuell durchgeführt werden.

Hinweise zum Installieren des Mac OS X-Agenten finden Sie unter "Verteilung auf Macintosh-, Linux- und UNIX-Clients" im *Installations- und Verteilungshandbuch*. Sobald Sie das Patch Manager-Add-on installiert haben, beinhaltet das Mac OS X-Agent-Standardpaket den Anfälligkeitsscanner. Wenn Sie den Mac OS X-Agenten vor dem Installieren von Patch Manager verteilt hatten, müssen Sie den Agenten erneut an die Clients verteilen, damit diese das aktualisierte Paket erhalten, das den Anfälligkeitsscanner beinhaltet.

So starten Sie den Anfälligkeitsscanner manuell

1. Öffnen Sie die **Systemeinstellungen** von MAC OS X und wählen Sie die Seite **LANDesk Client**.
2. Klicken Sie auf der Registerkarte **Übersicht** auf **Jetzt prüfen** im Abschnitt "Patch Manager".

Aktualisieren von Anfälligkeits- und Erkennungsregelinformationen

Ihr Netzwerk unterliegt ständig Sicherheitsbedrohungen durch neue Würmer und Viren sowie normale Wartungsaufgaben wie Softwareaktualisierungen und fehlerkorrigierte Programme. Jeden Tag kommt neue Hardware und Software auf den Markt, zusammen mit Patches, um unvermeidliche Anfälligkeiten zu reparieren. Der Patch Manager vereinfacht und beschleunigt den Prozess des Erfassens der neuesten bekannt gewordenen Anfälligkeit, Erkennungsregel und Patchdaten, indem Sie die Möglichkeit erhalten, Anfälligkeiten über eine LANDesk-gehostete Datenbank zu aktualisieren. Der LANDesk Patch Manager-Dienst konsolidiert bekannt gewordene Anfälligkeiten aus vertrauenswürdigen Quellen der Industrie und des Handels.

Patch Manager unterstützt zudem benutzerdefinierte Anfälligkeiten
Zusätzlich zu bekannten Anfälligkeiten können Sie eigene benutzerdefinierte Anfälligkeiten erstellen. Weitere Informationen finden Sie unter "Erstellen benutzerdefinierter Anfälligkeiten" weiter unten in diesem Kapitel.

Durch die Einrichtung und Verwaltung aktueller Anfälligkeitsinformationen und verknüpfter Patchinformationen können Sie Art und Umfang der Sicherheitsbedrohungen für jede unterstützte Plattform und Anwendung besser einschätzen. Sie können bestimmen, welche Anfälligkeiten für Ihre Umgebung relevant sind, und Anfälligkeitscan- und Reparaturaufgaben anpassen. Der erste Schritt besteht darin, immer über die neuesten bekannt gewordenen Anfälligkeitsinformationen zu verfügen.

Mit dem Patch Manager können Sie Anfälligkeitsaktualisierungen konfigurieren und sofort ausführen oder einen geplanten Anfälligkeitsaktualisierungstask erstellen, der zu einem bestimmten Zeitpunkt oder als wiederkehrender Task ausgeführt werden soll (siehe "Planen automatischer Anfälligkeitsaktualisierungen" weiter unten in diesem Kapitel).

Nur ein Management Suite Benutzer auf einem bestimmten Core Server (einschließlich zusätzlicher Konsolen) kann jeweils Anfälligkeiten aktualisieren. Wenn ein Benutzer versucht, Anfälligkeiten zu aktualisieren, während der Prozess bereits ausgeführt wird, wird eine Meldung angezeigt, die auf einen vorhandenen Konflikt hinweist.

So aktualisieren Sie Anfälligkeitsinformationen

1. Klicken Sie auf **Extras | Patch Manager**.
2. Klicken Sie auf die Schaltfläche **Anfälligkeitsinformationen aktualisieren** in der Symbolleiste.
3. Wählen Sie die Plattformen, deren Anfälligkeitsinformationen aktualisiert werden sollen. Sie können eine oder mehrere Plattformen aus der Liste wählen. Zu den verfügbaren Plattformen gehören: Windows, Mac und Sun Solaris. Je mehr Plattformen Sie auswählen, umso länger dauert die Aktualisierung.

4. Wählen Sie die Sprachen, deren Anfälligkeitsinformationen aktualisiert werden sollen. Sie können je nach den oben angegebenen Plattformen eine oder mehrere Sprachen aus der Liste auswählen. Je mehr Sprachen Sie auswählen, umso länger dauert die Aktualisierung. Eine ausführliche Beschreibung und Anleitung für diese Option finden Sie unter "Übersicht über die Option "Sprache neutral"" weiter unten in diesem Kapitel.
5. (Optional) Wenn neue Anfälligkeiten (d.h. Anfälligkeiten, die noch in keiner Anfälligkeitsgruppe im Patch Manager-Baum enthalten sind) automatisch in die Gruppe "Aktivierte Anfälligkeiten" aufgenommen werden sollen, anstatt am Standardspeicherort "Nicht zugewiesene Anfälligkeiten" abgelegt zu werden, aktivieren Sie das Kontrollkästchen **Neue Anfälligkeiten in die Gruppe "Aktiviert" verschieben**.
6. (Optional) Wenn Sie die aktuellen ausführbaren Patchdateien automatisch herunterladen möchten, aktivieren Sie das Kontrollkästchen **Verknüpfte Patches herunterladen** und klicken anschließend auf eine der Download-Optionen. Eine ausführliche Beschreibung dieser Optionen finden Sie unter "Übersicht über das Dialogfeld "Anfälligkeitseinstellungen aktualisieren"" weiter unten.

   - **Nur für erkannte Anfälligkeiten**
   - **Für alle Patches, auf die verwiesen wird**

   Die Patches werden heruntergeladen und an dem Speicherort abgelegt, der auf der Registerkarte "Patch" des Dialogfelds "Anfälligkeitseinstellungen aktualisieren" angegeben ist (siehe unten beschriebenen Vorgang).

7. (Optional) Wenn Ihr Netzwerk über einen Proxy-Server verfügt, der für externe Internet-Übertragungen verwendet wird (für die Aktualisierung der Anfälligkeitsdaten und heruntergeladenen Patches erforderlich), klicken Sie auf die Registerkarte **Proxy Server** und geben die Serveradresse, Port-Nummer und Berechtigungsnachweise an, wenn für den Zugriff auf den Proxy-Server eine Anmeldung erforderlich ist.
8. Klicken Sie auf **Übernehmen**, wenn Sie die Einstellungen speichern möchten.
9. Klicken Sie auf **Jetzt aktualisieren**, um die Anfälligkeitsaktualisierung auszuführen. Das Dialogfeld "Anfälligkeiten werden aktualisiert" zeigt den aktuellen Vorgang und dessen Status.
10. Wenn die Aktualisierung abgeschlossen ist, klicken Sie auf **Schließen**. Wenn Sie auf **Abbrechen** klicken, bevor die Aktualisierung abgeschlossen ist, werden nur die bis zu diesem Zeitpunkt verarbeiteten Daten in der Core-Datenbank gespeichert. Auf diese kann über das Patch Manager-Tool in der Konsole zugegriffen werden.

Hinweis: Schließen Sie die Management Suite-Konsole nicht, während ein Anfälligkeitsaktualisierungsprozess ausgeführt wird. Andernfalls wird der Prozess beendet. Dies gilt nicht für einen geplanten Task für die Aktualisierung von Anfälligkeitsinformationen.

So konfigurieren Sie den Speicherort für den Patchdownload

1. Klicken Sie im Dialogfeld "Anfälligkeitseinstellungen aktualisieren" auf die Registerkarte **Patch**.

2. Geben Sie einen UNC-Pfad für die kopierten Patchdateien an. Der Standardspeicherort ist das Verzeichnis \LDLogon\Patch des Core Servers.
3. Wenn der oben eingegebene UNC-Pfad zu einem anderen Speicherort als den Core Server führt, geben Sie einen gültigen Benutzernamen und ein Kennwort ein, um sich zu authentifizieren.
4. Geben Sie eine Web-URL-Adresse ein, über die Clients auf die heruntergeladenen Patches für die Verteilung zugreifen können. Die Web-URL-Adresse sollte dem oben angegebenen UNC-Pfad entsprechen.
5. Sie können auf **Testeinstellungen** klicken, um zu prüfen, ob mit der oben angegebenen Webadresse eine Verbindung hergestellt werden kann.
6. Wenn Sie den UNC-Pfad und die Web-URL-Adresse wieder auf die Standardeinstellung für den Speicherort zurücksetzen möchten, klicken Sie auf **Standardeinstellungen wiederherstellen**. Der Standardspeicherort ist das Verzeichnis \LDLogon\Patch des Core Servers.

Planen automatischer Anfälligkeitsaktualisierungen

Sie können Anfälligkeitsaktualisierungen auch als geplante Tasks konfigurieren, die zu einem bestimmten Zeitpunkt in der Zukunft oder als wiederkehrende Tasks ausgeführt werden. Dazu klicken Sie in der Symbolleiste auf die Schaltfläche **Periodische Aktualisierung planen**. Der Task "Anfälligkeitsinformationen aktualisieren" wird im Fenster "Geplante Tasks" erstellt. Legen Sie nun die Planoptionen fest.

Der Task "Anfälligkeitsinformationen aktualisieren" verwendet die aktuellen Einstellungen aus dem Dialogfeld "Anfälligkeitseinstellungen aktualisieren". Wenn Sie die Einstellungen für Plattform, Sprache, Patchdownload oder Proxy-Server für einen bestimmten Aktualisierungsauftrag ändern möchten, müssen Sie diese Einstellungen zuerst im Dialogfeld ändern, und zwar VOR dem Zeitpunkt, zu dem die Ausführung des Task geplant ist.

Übersicht über das Dialogfeld "Anfälligkeitseinstellungen aktualisieren"

In diesem Dialogfeld konfigurieren Sie die Einstellungen für Anfälligkeitsaktualisierungen, den Speicherort für Patchdownloads und die Proxy-Server-Informationen.

Hinweis: Wenn der Task "Anfälligkeitsinformationen aktualisieren" ausgeführt wird, werden die derzeit aktuellen Einstellungen aus diesem Dialogfeld verwendet, nicht jedoch die Einstellungen zum Zeitpunkt der Task-Erstellung. Die aktuellen Einstellungen aus diesem Dialogfeld werden von jedem Task zur Aktualisierung der Anfälligkeitsinformationen verwendet, wenn der Task ausgeführt wird. Außerdem werden die aktuellen Speicherorteinstellungen für den Patchdownload verwendet, die sich beim Herunterladen eines Patches auf der Registerkarte "Patch" dieses Dialogfelds befinden.

Wenn Sie die Änderungen speichern möchten, die Sie auf einer Registerkarte dieses Dialogfeldes vorgenommen haben, klicken Sie auf **Übernehmen**. Wenn Sie auf **Schließen** klicken, werden die Änderungen nicht gespeichert.

Dieses Dialogfeld enthält drei Registerkarten:

Registerkarte "Download"

- **Plattformen zur Aktualisierung auswählen:** Legt fest, welche Anfälligkeiten welcher Plattform aktualisiert werden. Sie können eine oder mehrere Plattformen auswählen.
- **Sprachen zur Aktualisierung auswählen:** Legt die Sprachversionen der Anfälligkeiten der ausgewählten Plattformen fest, die aktualisiert werden.

  Übersicht über die Option "Sprache neutral":
  Manche Anfälligkeiten und verknüpfte Patches sind sprachneutral oder unabhängig, d.h. sie sind mit jeder Sprachversion des Betriebssystems oder der Anwendung kompatibel, das/die von der Anfälligkeit und dem Patch betroffen ist. Sie benötigen also kein separates sprachenspezifisches Patch, um diese Anfälligkeiten zu reparieren, da der Patch alle unterstützten Sprachen abdeckt. Linux/UNIX-Plattformen wie Sun Solaris verwenden beispielsweise nur sprachneutrale Anfälligkeiten/Patches. Microsoft Windows arbeitet überwiegend mit sprachspezifischen Anfälligkeiten/Patches, aber es gibt auch ein paar sprachneutrale.

  Wenn Sie die Windows-Plattform ausgewählt haben, können Sie die Sprachen auswählen, deren Anfälligkeitsinformationen aktualisiert werden sollen. (Sie können auch die Sprache neutral auswählen, wenn Sie sprachübergreifende Anfälligkeiten für Windows aktualisieren möchten und sofern diese verfügbar sind.)

  Wenn Sie die Plattform Sun Solaris gewählt haben, MÜSSEN Sie die Option "Sprache neutral" auswählen. Andernfalls werden die Anfälligkeitsinformationen für diese Plattform nicht aktualisiert. Wenn Sie bestimmte Sprachen für diese Plattform auswählen, wirkt sich dies nicht auf die Anfälligkeitsaktualisierung aus.

- **Neue Anfälligkeiten in die Gruppe "Aktivierte Anfälligkeiten" verschieben:** Neue Anfälligkeiten werden automatisch in die Gruppe "Aktivierte Anfälligkeiten" und nicht in die Standardgruppe "Nicht zugewiesene Anfälligkeiten" verschoben.
- **Verknüpfte Patches herunterladen:** Ausführbare Patchdateien werden automatisch an den angegebenen Speicherort für Downloads heruntergeladen (siehe Registerkarte "Patch"). Dabei wird eine der folgenden Downloadoptionen berücksichtigt:

  - **Nur für erkannte Anfälligkeiten:** Es werden nur die Patches heruntergeladen, die mit Anfälligkeiten verknüpft sind, die beim letzten Anfälligkeitsscan erkannt wurden (z.B. die Anfälligkeiten, die sich derzeit in der Gruppe "Erkannte Anfälligkeiten" befinden).
  - **Für alle Patches, auf die verwiesen wird:** Es werden ALLE Patches heruntergeladen, die mit Anfälligkeiten verknüpft sind, die sich derzeit in der Gruppe "Aktivierte Anfälligkeiten" befinden.

Registerkarte "Patch"

- **UNC-Pfad, in den der Core Dateien schreibt:** Gibt an, wohin die Patchdateien heruntergeladen werden. Der Standardspeicherort ist der Ordner \LDLogon\Patch des Core Servers. Sie können einen anderen UNC-Pfad für das Herunterladen von Patches eingeben. Dabei müssen Sie jedoch sicherstellen, dass ein Zugriff auf den Speicherort erfolgen kann, indem Sie gültige Berechtigungsnachweise für die Authentifizierung in die unten stehenden Felder eingeben.
- **Berechtigungsnachweise zum Speichern von Patches:** Enthält einen gültigen Benutzernamen und ein Kennwort für den Zugriff auf einen anderen Speicherort als den Core Server.
- **Web-URL für den Zugriff der Clients auf die Daten:** Nennt eine Webadresse, auf welche die Clients zugreifen können, um die heruntergeladenen Patches zu verteilen. Der Standardspeicherort ist der Ordner \LDLogon\Patch des Core Servers. Dieser Speicherort entspricht in der Regel dem oben angegebenen UNC-Pfad.
- **Testeinstellungen:** Führt einen Verbindungstest mit der angegebenen Web-URL-Adresse aus.
- **Auf Standard zurücksetzen:** Setzt den UNC-Pfad und die Web-URL-Adresse auf den Standardspeicherort zurück, der dem Ordner \LDLogon\Patch des Core Servers entspricht.

Registerkarte "Proxy-Server"

Wenn Ihr Netzwerk einen Proxy-Server für externe Übertragungen (wie z.B. Internetzugriff) nutzt, aktivieren und konfigurieren Sie auf dieser Registerkarte die Proxy-Server-Einstellungen. Für die Aktualisierung der Anfälligkeitsinformationen und zum Herunterladen der Patchdateien vom entsprechenden Webdienst ist ein Internetzugang erforderlich.

- **Proxy-Server verwenden: Aktiviert die Proxy-Server-Option (die Option ist standardmäßig deaktiviert). Wenn Sie einen Proxy-Server aktivieren, müssen Sie die Adresse und den Port in die unten stehenden Felder eingeben.**
- **Server:**
  - **Adresse:** Gibt die IP-Adresse Ihres Proxy-Servers an.
  - **Port:** Gibt die Portnummer Ihres Proxy-Servers an.
- **HTTP-basierter Proxy:**Aktiviert den Proxy-Server, wenn es sich um einen HTTP-basierten Proxy handelt (wie z.B. Squid), damit der Server Verbindungen mit FTP-Sites herstellen und von diesen Sites Patches herunterladen kann. (Auf bestimmten FTP-Sites gehostete Patches können erst dann über einen HTTP-basierten Proxy heruntergeladen werden, wenn Sie zuvor diese Option aktivieren.)
- **Erfordert Anmeldung:** Ermöglicht die Eingabe eines Benutzernamens und eines Kennworts, wenn der Proxy-Server Berechtigungsnachweise verlangt und kein transparenter Proxy-Server ist.
  - **Benutzername:** Geben Sie einen gültigen Benutzernamen und Berechtigungsnachweise für die Authentifizierung beim Proxy-Server ein.
  - **Kennwort:** Geben Sie das Kennwort des Benutzers ein.

Erstellen benutzerdefinierter Anfälligkeits- und Erkennungsregeln

Zusätzlich zu den bekannt gewordenen Anfälligkeiten, die Sie über den LANDesk Patch Manager-Dienst aktualisieren, können Sie auch eigene benutzerdefinierte (oder angepasste) Anfälligkeiten erstellen—einschließlich benutzerdefinierter Erkennungsregeln, verknüpfter Patchdateien und spezieller Zusatzbefehle, die eine erfolgreiche Reparatur gewährleisten.

Schwachstellen bestehen aus einer eindeutigen Kennung, Titel, Datum der Veröffentlichung, Sprache und anderen Identifizierungsdaten sowie der/den Erkennungsregel(n), die dem Anfälligkeitsscanner mitteilen, wonach er auf Zielclients suchen soll. Erkennungsregeln definieren die bestimmte Plattform, Anwendung, Datei oder die bestimmten Registrierungsbedingungen, nach der/denen der Anfälligkeitsscanner sucht, um eine Anfälligkeit (oder praktisch jede *beliebige* Systembedingung bzw. jeden beliebigen Systemstatus) auf gescannten Clients ausfindig zu machen.

Die benutzerdefinierten Anfälligkeiten des Patch Manager sind eine leistungsstarke, flexible Funktion, mit der Sie eine zusätzliche Eigentümer-basierte Ebene der Patchsicherheit auf Ihrem System realisieren können. Zusätzlich zur Verbesserung der Patchsicherheit und anderen innovativen Tasks, die die Vorteile der Scanningfunktionen des Anfälligkeitsscanners nutzen, können benutzerdefinierte Anfälligkeiten u.a. auch dazu verwendet werden, Systemkonfigurationen zu bewerten, nach bestimmten Datei- und Registrierungseinstellungen zu suchen und Anwendungsaktualisierungen zu verteilen.

Benutzerdefinierte Anfälligkeiten müssen nicht notwendigerweise Reparaturaktionen (Verteilen und Installieren von Patchdateien) ausführen. Wenn die benutzerdefinierte Anfälligkeit mit einer "Nur erkennen"-Erkennungsregel bzw. -Erkennungsregeln definiert ist, werden Zielgeräte vom Anfälligkeitsscanner gescannt und die Geräte gemeldet, auf die die vorgeschriebene Bedingung der Regel (oder "Anfälligkeit") gefunden wurde. Sie können beispielsweise eine nur auf die Erkennung begrenzte benutzerdefinierte Regel für den Anfälligkeitsscanner schreiben, mit der verwaltete Geräte auf Folgendes geprüft werden können:

- Anwendung: %s
- Datei: %s
- Dateiversion
- Paketspeicherort:
- Dateidatum
- Registrierungseinstellung
- Und mehr...

Sie können so viele benutzerdefinierte Anfälligkeiten erstellen, wie Sie für das Einrichten und Warten einer sicheren Patchumgebung benötigen.

So erstellen Sie eine benutzerdefinierte Anfälligkeit

1. Klicken Sie auf **Extras | Patch Manager**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Anfälligkeit erstellen**. Es wird eine editierbare Version des Dialogfelds "Anfälligkeitseigenschaften" geöffnet. In diesem Dialogfeld können Sie Anfälligkeitseigenschaften nach Bedarf festlegen.
3. Geben Sie eine eindeutige Kennung für die Anfälligkeit ein. (Der vom System generierte Erkennungscode kann bearbeitet werden.)
4. Das Datum der Veröffentlichung ist das aktuelle Datum und kann nicht geändert werden.
5. Geben Sie einen beschreibenden Titel für die Anfälligkeit ein. Dieser Titel wird in der Anfälligkeitsliste angezeigt.
6. Geben Sie den Schweregrad an. Zu den verfügbaren Optionen gehören: Unbekannt, Service Pack, Kritisch, Hoch, Mittel, Niedrig und Nicht anwendbar.
7. Geben Sie den Status der Anfälligkeit ein. Zu den verfügbaren Optionen gehören: Deaktiviert, Aktiviert und Nicht zugewiesen. Wenn Sie einen Status angeben, wird die Anfälligkeit in die entsprechende Gruppe in der Patch Manager-Baumansicht eingefügt (siehe "Hauptansicht" weiter oben in diesem Kapitel).
8. Die Spracheinstellung für benutzerdefinierte Anfälligkeiten ist automatisch auf INTL (international oder sprachneutral) eingestellt. Dies bedeutet, dass die Anfälligkeit auf jede Sprachversion des Betriebssystems und/oder der Anwendungen angewendet werden kann.
9. Die Liste "Erkennungsregeln" zeigt alle Regeln an, die von dieser Anfälligkeit verwendet werden. Wenn Sie eine neue benutzerdefinierte Anfälligkeit erstellen, sollten Sie mindestens eine Erkennungsregel definieren, die für das Scannen nach dieser Anfälligkeit eingesetzt wird. Klicken Sie auf **Hinzufügen**, um Erkennungsregeln hinzuzufügen. (Lesen Sie hierzu die Schritt-für-Schritt-Anleitungen weiter unten).
10. Wenn Sie zusätzliche Informationen zu dieser Anfälligkeit bereitstellen möchten, klicken Sie auf die Registerkarte **Beschreibung** und geben Ihre Kommentare in das Textefeld und/oder eine gültige Webadresse ein, auf der weitere Informationen zu finden sind.

Wie bei den bekannt gewordenen Anfälligkeiten der Hersteller sollten auch benutzerdefinierte Anfälligkeiten eine oder mehrere Erkennungsregeln beinhalten, die dem Anfälligkeitsscanner mitteilen, nach welchen Bedingungen auf verwalteten Geräten gesucht werden sollte. Führen Sie die nachstehend beschriebenen Schritte aus, um eine Erkennungsregel für eine benutzerdefinierte Anfälligkeit zu erstellen.

So erstellen Sie eine benutzerdefinierte Erkennungsregel

1. Klicken Sie mit der rechten Maustaste auf eine benutzerdefinierte Anfälligkeit und klicken Sie dann auf **Eigenschaften**. (Oder doppelklicken Sie auf die Anfälligkeit.)
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, die sich unter der Liste "Erkennungsregeln" befindet. Eine editierbare Version des Dialogfelds "Regeleigenschaften" wird geöffnet und gibt Ihnen die Möglichkeit, eine Erkennungsregel zu konfigurieren.
3. Geben Sie einen eindeutigen Namen für die Regel ein.

4. Der Regelstatus lässt sich hier nicht bearbeiten. Um den Status einer Erkennungsregel zu ändern, klicken Sie in einer der Listenansichten mit der rechten Maustaste auf die Regel. Klicken Sie dann, je nach aktuellem Status, auf **Aktivieren** oder **Deaktivieren**.
5. Geben Sie durch Auswahl der Option **Sanierungsziel** oder **Nur erkennen** an, ob die Regel Anfälligkeiten reparieren oder nur erkennen soll. Damit Sie nach Bedarf veranlassen können, dass eine Regel eine Anfälligkeit sowohl repariert als auch erkennt, konvertiert das System die Felder in der Patchdatei in editierbare Felder und blendet die Registerkarte "Befehle" ein.
6. Wenn Sie "Sanierungsziel" ausgewählt haben, geben Sie den Patch-Dateinamen und die URL zu dieser Datei ein.

   Sie können versuchen, die verknüpfte Patchdatei herunterzuladen, indem Sie auf **Downloaden** klicken; oder Sie können die Datei zu einem späteren Zeitpunkt herunterladen.

   Was Regeln betrifft, die das Reparieren von Anfälligkeiten einschließen, so wird dringend empfohlen, ein Hash für die Patchdatei zu erstellen, indem Sie auf **MD5-Hash generieren** klicken. Die eigentliche Patchdatei muss heruntergeladen werden, bevor Sie ein Hash erstellen können. Weitere Informationen zur Verwendung eines Hash finden Sie unter "Erkennungsregel: Registerkarte "Allgemein"" weiter unten in diesem Kapitel.

6. Wählen Sie die Plattform(en) aus, auf denen der Anfälligkeitsscanner für die Suche nach der Anfälligkeit dieser Erkennungsregel ausgeführt werden soll. Welche Plattformen als verfügbar in der Liste angezeigt werden, ist davon abhängig, welche Anfälligkeiten Sie mithilfe des LANDesk Patch Manager-Dienstes aktualisiert haben. Sie müssen mindestens eine Plattform auswählen.
7. Um die Regel mit einer oder mehreren Softwareanwendungen zu verknüpfen, klicken Sie auf die Registerkarte **Produkte** und dann auf **Bearbeiten**, um ein Dialogfenster zu öffnen, in dem Sie Produkte zur Liste "Verknüpfte Produkte" hinzufügen oder aus dieser Liste entfernen können. Welche Produkte als verfügbar in der Liste angezeigt werden, ist davon abhängig, welche Anfälligkeiten Sie mithilfe des LANDesk Patch Manager-Dienstes aktualisiert haben. Sie müssen nicht unbedingt ein Produkt mit einer Erkennungsregel verknüpfen. Verknüpfte Produkte fungieren als Filter während des Anfälligkeitsscans. Wenn das angegebene verknüpfte Produkt auf dem Client gefunden wird, wird der Anfälligkeitsscan beendet. Wird das Produkt jedoch gefunden oder wurden keine Produkte angegeben, so setzt der Scanner die Dateiprüfung fort.
8. Um bestimmte Dateibedingungen zu konfigurieren, nach denen die Regel scannen soll, klicken Sie auf die Registerkarte **Dateien** und dann auf **Hinzufügen**, um die Felder auf dieser Registerkarte editierbar zu machen. Der erste Schritt beim Konfigurieren einer Dateibedingung ist das Festlegen der Überprüfungsmethode. Die ausgewählte Überprüfungsmethode bestimmt, welche Felder auf dieser Registerkarte angezeigt werden. Zum Speichern einer Dateibedingung klicken Sie auf **Aktualisieren**. Sie können so viele Dateibedingungen hinzufügen, wie Sie möchten. Eine ausführliche Beschreibung dieser Option finden Sie unter unter "Erkennungsregel: Registerkarte "Dateien"" weiter unten in diesem Kapitel.

9. Um bestimmte Registrierungsbedingungen zu konfigurieren, nach denen die Regel scannen soll, klicken Sie auf die Registerkarte **Registrierung** und dann auf **Hinzufügen**, um die Felder editierbar zu machen. Zum Speichern einer Registrierungsbedingung klicken Sie auf **Aktualisieren**. Sie können so viele Registrierungsbedingungen hinzufügen, wie Sie möchten. Eine ausführliche Beschreibung dieser Option finden Sie unter unter "Erkennungsregel: Registerkarte "Registrierung"" weiter unten in diesem Kapitel.
10. Um zusätzliche Kommentare hinzuzufügen, klicken Sie auf die Registerkarte **Kommentare** und geben den gewünschten Text ein.
11. Wenn Sie (in Schritt 5) die Option "Sanierungsziel" für diese Regel ausgewählt haben, können Sie zusätzliche Befehle konfigurieren, die die Anfälligkeiten auf den betroffenen Clients reparieren. Um einen zusätzlichen Sanierungsbefehl zu konfigurieren, klicken Sie auf die Registerkarte **Befehle** und dann auf **Hinzufügen**, um einen Befehlstyp auszuwählen und um die Argumentfelder des Befehls editierbar zu machen. Zusätzliche Befehle sind nicht erforderlich. Wenn Sie keine speziellen Befehle konfigurieren, wird die Patchdatei nur für sich ausgeführt, wie dies normalerweise der Fall ist. Eine ausführliche Beschreibung dieser Option finden Sie unter unter "Erkennungsregel: Registerkarte "Befehle"" weiter unten in diesem Kapitel.

Nachdem Sie nun einen benutzerdefinierte Anfälligkeit erstellt haben, können Sie diese Anfälligkeit genauso bearbeiten wie eine bekannte Anfälligkeit eines Herstellers oder Anbieters. Sie können den Status der Anfälligkeiten auf "Aktiviert" setzen oder die Anfälligkeit zu der Gruppe "Aktivierte Anfälligkeiten" hinzufügen, die vom nächsten Anfälligkeitsscan erfasst werden soll. Sie können die Anfälligkeit zudem in die Gruppe "Deaktiviert" oder "Nicht zugewiesen" einfügen, betroffene Computer anzeigen, die Option "Automatisches Korrigieren" aktivieren, einen Reparaturauftrag erstellen oder den Scan-/Reparaturstatus löschen. Wählen Sie die betreffende Option aus, indem Sie durch Klicken mit der rechten Maustaste auf eine benutzerdefinierte Anfälligkeit das Kontextmenü für diese Anfälligkeit öffnen.

Zwei Optionen, die nur für benutzerdefinierte Anfälligkeiten angeboten werden, sind "Importieren/Exportieren" und "Löschen".

Importieren und Exportieren benutzerdefinierter Anfälligkeiten

Patch Manager bietet eine Möglichkeit, benutzerdefinierte Anfälligkeiten und Erkennungsregeldefinitionen zu importieren und exportieren. Sie können keine bekannt gewordenen Anfälligkeiten in Programmen importieren oder exportieren.

Anfälligkeitsdefinitionen werden als XML-Datei exportiert und importiert.

Das Importieren und Exportieren ist nützlich, wenn Sie benutzerdefinierte Anfälligkeiten anderen Core Server zur Verfügung stellen möchten. Das Exportieren bietet Ihnen die Möglichkeit, eine Sicherungskopie von einer Anfälligkeitsdefinition zu speichern, die Sie vorübergehend aus der Core-Datenbank entfernen möchten.

Sie können die Export-/Importfunktion auch dazu verwenden, eine Anfälligkeit zu exportieren, die exportierte Datei manuell als Vorlage zu bearbeiten, mehrere Varianten der Anfälligkeit zu speichern und dann die neuen Anfälligkeitsdefinitionen zu importieren. Wenn es sich um eine komplexe Anfälligkeit handelt, ist dieses Vorgehen möglicherweise schneller und einfacher als das Erstellen mehrerer Definitionen in der Konsole.

So exportieren Sie eine benutzerdefinierte Anfälligkeit

1. Wählen Sie von einer Liste mit Anfälligkeiten in Patch Manager eine oder mehrere benutzerdefinierte Anfälligkeiten aus.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Exportieren**. (Alternativ dazu können Sie auch mit der rechten Maustaste auf die ausgewählten Anfälligkeiten und dann auf **Exportieren** klicken.)
3. Geben Sie den Pfad zu dem Ordner ein, aus dem Sie die Anfälligkeit als eine XML-Datei exportieren möchten.
4. Wenn Sie die Anfälligkeit zu einem früheren Zeitpunkt in den angegebenen Speicherort exportiert hatten und sie jetzt überschreiben möchten, klicken Sie auf **Vorhandene Anfälligkeiten überschreiben**.
5. Klicken Sie auf **Exportieren**. Überprüfen Sie im Fenster "Exportstatus", ob die Anfälligkeit erfolgreich exportiert wurde.

   Eine exportierte Anfälligkeit bleibt weiterhin in der Core-Datenbank bestehen und wird deshalb auch nach wie vor in der Gruppe "Benutzerdefinierte Anfälligkeiten" sowie in der Gruppe, die ihrem Status entspricht, angezeigt: Nicht zugewiesen, Aktiviert oder Deaktiviert.

6. Klicken Sie auf **Schließen**.

So importieren Sie eine benutzerdefinierte Anfälligkeit

1. Klicken Sie im Fenster "Patch Manager" auf die Schaltfläche **Importieren** der Symbolleiste.
2. Suchen und wählen Sie eine oder mehrere Anfälligkeitsdefinitionen (XML-Datei), die Sie importieren möchten, und klicken Sie dann auf **Öffnen**. Wenn die Anfälligkeit bereits in der Core-Datenbank existiert, werden Sie gefragt, ob Sie sie überschreiben möchten. Überprüfen Sie im Statusfenster, ob die Anfälligkeit erfolgreich importiert wurde.
3. Klicken Sie auf **Schließen**. Importierte Anfälligkeiten (neue und aktualisierte) werden in die Gruppe "Benutzerdefinierte Anfälligkeiten" und in die Gruppe, die dem Status der Anfälligkeit entspricht, eingefügt.

Löschen benutzerdefinierter Anfälligkeiten

Wenn eine benutzerdefinierte Anfälligkeit nicht mehr benötigt wird, können Sie sie löschen. Beim Löschen der benutzerdefinierten Anfälligkeit wird ihre Definition, einschließlich aller ihr zugeordneten Erkennungsregeln, aus der Core-Datenbank und dem Patch Manager-Fenster gelöscht. Die eigentlichen Anfälligkeitsinformationen werden beim Exportieren nicht entfernt.

Wie beim Löschen der Informationen bekannter Anfälligkeiten der Standard-Industrieprogramme werden auch beim Löschen benutzerdefinierter Anfälligkeiten keine heruntergeladenen, auf die Anfälligkeit bezogene Patchdateien entfernt.

Um benutzerdefinierte Anfälligkeiten zu löschen, wählen Sie eine oder mehrere benutzerdefinierte Anfälligkeiten aus und klicken dann auf die Schaltfläche **Benutzerdefinierte Anfälligkeiten löschen** in der Symbolleiste.

Wiederherstellen benutzerdefinierter Anfälligkeiten, die exportiert wurden
Wenn Sie eine Definition für eine benutzerdefinierte Anfälligkeit löschen, die zuvor als XML-Datei exportiert worden war, können Sie diese Anfälligkeit wiederherstellen, indem Sie sie mithilfe des Importwerkzeugs wieder in Patch Manager importieren.

Anzeigen von Anfälligkeits- und Erkennungsregelinformationen

Nachdem Anfälligkeiten mit den neuesten Informationen aus dem LANDesk Patch Manager-Dienst aktualisiert wurden, können Sie Anfälligkeiten und Erkennungsregeln in ihren jeweiligen Gruppen im Patch Manager-Fenster anzeigen, nach Plattform und Produkt sortiert auflisten, in verschiedene Statusgruppen verschieben oder in Ihre eigenen benutzerdefinierten Gruppen kopieren. Informationen über die verschiedenen Gruppen in der Patch Manager-Ansicht und über deren Verwendung finden Sie unter "Informationen zum Patch Manager-Fenster" weiter unten in diesem Kapitel

Sie können die Eigenschaften der einzelnen aktualisierten Anfälligkeiten und Erkennungsregeln betrachten, indem Sie mit der rechten Maustaste auf ein Element klicken und **Eigenschaften** auswählen. Anhand dieser Informationen können Sie bestimmen, welche Anfälligkeiten für die von Ihrem Netzwerk unterstützten Plattformen und Anwendungen von Belang sind, wie die Erkennungsregeln einer Anfälligkeit eine Anfälligkeit ausfindig machen, welche Patches verfügbar sind und wie Sie die Sanierungsmaßnahmen für die betroffenen Clients konfigurieren und ausführen sollten.

Benutzerdefinierte Anfälligkeiten können bearbeitet werden
Wenn Sie eine in der Industrie bekannt gewordene Anfälligkeit auswählen, dient das Dialogfenster, in dem die Eigenschaften dieser Anfälligkeit angezeigt werden, in erster Linie Informationszwecken. Wählen Sie hingegen eine benutzerdefinierte Anfälligkeit aus oder erstellen Sie eine benutzerdefinierte Anfälligkeit, sind die Felder im Dialogfeld "Eigenschaften" editierbar. Dadurch erhalten Sie die Möglichkeit, die Anfälligkeit und ihre Erkennungsregel(n) zu definieren.

Sie können auch die Anfälligkeits- und Erkennungsregelinformationen zu (einem) bestimmten überprüften Gerät(en) direkt in der Netzwerkansicht anzeigen, indem Sie ein oder mehrere ausgewählte(s) Gerät(e) mit der rechte Maustaste anklicken und dann auf **Anfälligkeitsinformationen** klicken.

Informationen zum Dialogfeld "Anfälligkeitseigenschaften"

Verwenden Sie dieses Dialogfeld zum Anzeigen der Eigenschaften einer heruntergeladenen Anfälligkeit oder zum Erstellen und Bearbeiten benutzerdefinierter Anfälligkeiten.

Diese Informationen sind für Anfälligkeiten, die über den Patch Manager-Dienst heruntergeladen wurden (siehe "Aktualisieren von Anfälligkeitsinformationen" weiter oben in diesem Kapitel), schreibgeschützt.

Im Falle einer benutzerdefinierten Anfälligkeit sind die Felder in diesem Dialogfeld editierbar. Sie können Anfälligkeitseinstellungen definieren und in die auf der jeweiligen Registerkarte verfügbaren Felder Informationen eingeben, um eigene Anfälligkeitsdefinitionen zu erstellen (siehe "Erstellen einer benutzerdefinierten Anfälligkeit" weiter oben in diesem Kapitel).

Mit den Schaltflächen, auf denen nach links und rechts zeigende Pfeile abgebildet sind (<, >), können Sie Informationen zu den Eigenschaften der vorherigen bzw. nächsten Anfälligkeit anzeigen, wobei die Anfälligkeiten in der Reihenfolge erscheinen, in der sie aktuell im Hauptfenster aufgelistet sind.

Dieses Dialogfeld enthält zwei Registerkarten:

Register "Allgemein"

- **Anfälligkeitskennung** Gibt den eindeutigen, vom Anbieter definierten (oder benutzerdefinierten) alphanumerischen Code der Anfälligkeit an.
- **Veröffentlichungsdatum:** Gibt das Datum an, an dem die Anfälligkeit vom Anbieter veröffentlicht (oder von einem Benutzer erstellt) wurde.
- **Titel:** Beschreibt die Art oder das Ziel der Anfälligkeit in einem kurzen Text.
- **Schweregrad:** Gibt den Schweregrad der Anfälligkeit gemäß einer unabhängigen Bewertung an (oder wie von dem Benutzer angegeben, der die benutzerdefinierte Anfälligkeit erstellt hat). Mögliche Schweregrade sind folgende: Service Pack, Kritisch, Hoch, Mittel, Niedrig, Nicht anwendbar und Unbekannt.
- **Status:** Gibt den Status der Anfälligkeit im Patch Manager-Fenster an. Die drei Statusindikatoren sind folgende: "Aktiviert" bedeutet, dass die Anfälligkeit für den nächsten Anfälligkeitsscan auf Geräten aktiviert wurde; "Deaktiviert", dass sie nicht in den Scan einbezogen wird; "Nicht zugewiesen", dass sie nicht gescannt wird und sich in einem temporären Wartebereich befindet. Weitere Informationen zu den drei Statusmöglichkeiten bzw. Gruppen finden Sie unter "Informationen zum Patch Manager-Fenster" weiter oben in diesem Kapitel.
- **Sprache:**Gibt die Sprache der Plattform an, für die die Anfälligkeit den Scan ausführen soll. INTL ist der Standardwert für benutzerdefinierte Anfälligkeiten; er ist mit allen Sprachen kompatibel und kann nicht geändert werden.
- **Erkennungsregeln:**Zeigt die mit der Anfälligkeit verknüpften Erkennungsregeln. Beachten Sie, dass der Eintrag **Heruntergeladen** angibt, ob die Patchdatei in die lokale Ablage heruntergeladen wurde, und dass **Unbeaufsichtigte Installation** angibt, ob der Patch auf den Clients ohne Benutzerbeteiligung installiert wird. Sie können direkt von dieser Ansicht aus mit der rechten Maustaste auf eine Regel klicken, um ein Patch herunterzuladen oder die Regel zu deaktivieren/aktivieren. Doppelklicken Sie auf die Regel, um ihre Eigenschaften anzuzeigen.

  Hinweis: Sie können beim Anzeigen einer benutzerdefinierten Anfälligkeit auf **Hinzufügen** klicken, um eine neue Erkennungsregel zu erstellen (siehe "Erstellen einer benutzerdefinierten Erkennungsregel" weiter oben in diesem Kapitel); oder Sie können auf **Bearbeiten** klicken, um die ausgewählte Regel zu bearbeiten bzw. auf **Löschen**, um sie zu entfernen.

Registerkarte "Beschreibung"

- **Beschreibung:** Stellt zusätzliche Details zur Anfälligkeit bereit. Diese Informationen werden den Entwicklungs- und Testhinweisen des Anbieters entnommen (oder sie werden von dem Benutzer zur Verfügung gestellt, der die Anfälligkeit definiert hat).
- **Weitere Infos:** Enthält einen HTTP-Link auf eine anbieterspezifische (oder benutzerdefinierte) Webseite, für gewöhnlich eine Support-Site, die weitere Informationen zur Anfälligkeit enthält.

Informationen zum Dialogfeld "Erkennungsregeleigenschaften"

Verwenden Sie dieses Dialogfeld zum Anzeigen der Eigenschaften von Erkennungsregeln für heruntergeladene Anfälligkeiten oder zum Erstellen und Bearbeiten von Erkennungsregeln benutzerdefinierter Anfälligkeiten.

Diese Informationen sind für Erkennungsregeln, die zu heruntergeladenen Anfälligkeiten gehören, schreibgeschützt.

Für die Erkennungsregel einer benutzerdefinierten Anfälligkeit sind die Felder in diesem Dialogfeld editierbar. Zum Erstellen benutzerdefinierter Erkennungsregeln können Sie Einstellungen für Erkennungsregeln definieren und Informationen in die Felder auf der jeweiligen Registerkarte eingeben. Wenn Sie für diese Regel "Sanierungsziel" ausgewählt haben, wird zusätzlich die Registerkarte "Befehle" eingeblendet, um Ihnen die Möglichkeit zur Definition zusätzlicher, während der Sanierung auszuführender Befehle zu geben.

Mit den Schaltflächen, auf denen nach links und rechts zeigende Pfeile abgebildet sind (<, >), können Sie Informationen zu den Eigenschaften der vorherigen bzw. nächsten Erkennungsregel anzeigen, wobei diese in der Reihenfolge erscheinen, in der sie aktuell im Hauptfenster aufgelistet sind.

Dieses Dialogfeld enthält fünf (oder sechs) Registerkarten:

Register "Allgemein"

- **Regelname:** Zeigt den Namen der Erkennungsregel an.
- **Status:** Gibt an, ob die Erkennungsregel aktiviert oder deaktiviert ist. Diese beiden Zustände entsprechen den Gruppen "Aktivierte Erkennungsregeln" und "Deaktivierte Erkennungsregeln" im Patch Manager-Fenster. Aktivierte Regeln können zum Scannen verwendet werden, deaktiverte Regeln dagegen nicht.
- **"Sanierungsziel" oder "Nur erkennen":** Gibt an, ob die Erkennungsregel lediglich prüft, ob die verknüpfte Anfälligkeit existiert ("Nur erkennen"), oder ob sie eine erkannte Anfälligkeit auch saniert.
- **Name der Patchdatei: Zeigt den Namen der Patchdatei, die zur Sanierung der Anfälligkeit, wenn sie erkannt wird, erforderlich ist. Für benutzerdefinierte "Nur erkennen"-Regeln wird keine Patchdatei benötigt. (Beachten Sie, dass eine Patchdatei für benutzerdefinierte Anfälligkeiten eine ausführbare Datei, eine Textdatei eine Zip-Datei sein kann, je nachdem, welches Sanierungsverfahren Sie ausgewählt haben.)**
- **Patch-URL:** Zeigt den HTTP-Pfad an, von dem die Patchdatei heruntergeladen werden kann.

Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, die auch zur Sanierung verwendet wird, und Sie haben einen Patch-Dateinamen und eine URL eingegeben, können Sie auf **Downloaden**klicken, um zu versuchen, die Patchdatei herunterzuladen. Sie können die Patchdatei jedoch auch zu einem späteren Zeitpunkt herunterladen.

Beim Herunterladen der Patchdatei empfiehlt LANDesk ausdrücklich, einen Hash für die Patchdatei zu erstellen, indem Sie auf **MD5-Hash generieren** klicken. (Die meisten, wenn nicht alle, Patchdateien, die mit einer bekannten Anfälligkeit verknüpft sind, sollten einen Hash besitzen.) Die Patchdatei muss heruntergeladen werden, bevor Sie ein Hash erstellen können. Eine Hash-Datei wird auch verwendet, um die Integrität der Patchdatei während der Sanierung (d.h., wenn die Patchdatei auf den betroffenen Client verteilt und installiert wird) zu gewährleisten. Der Anfälligkeitsscanner vergleicht hierfür den Hash-Code, den Sie beim Klicken auf die Schaltfläche "MD5-Hash erstellen" erstellt haben, mit dem neuen Hash, den er ummittelbar vor dem Versuch, die Patchdatei aus dem Patchreservoir auf dem Client zu installieren, erstellt hat. Wenn die beiden Hash-Dateien identisch sind, wird die Sanierung fortgesetzt. Wenn die beiden Hash-Dateien nicht übereinstimmen, d.h. die Patchdatei irgendwie seit dem Herunterladen in das Reservoir geändert wurde, wird der Sanierungsvorgang eingestellt.

- **Anfälligkeit:** Zeigt die Kennung und den Titel der Anfälligkeit an, mit der die Regel verknüpft ist.
- **Betroffene Plattformen:** Identifiziert das/die Betriebssystem(e), auf denen der Anfälligkeitsscanner ausgeführt wird, um nach der Anfälligkeit für die Regel zu suchen. Wenigstens eine Plattform muss ausgewählt werden. Wenn ein Zielgerät ein anderes Betriebssystem ausführt, wird der Anfälligkeitsscan abgebrochen.

Registerkarte "Produkte"

- **Betroffene Produkte:** Listet die mit der Erkennungsregel verbundenen Produkte auf. Wählen Sie ein Produkt in der Liste aus, um den Namen, Anbieter und die Versionsinformationen des Produkts anzuzeigen.

Wenn Sie eine benutzerdefinierte Regel erstellen oder bearbeiten, können Sie auf **Bearbeiten** klicken, um Produkte zu dieser Liste hinzuzufügen oder daraus zu entfernen. Welche Produkte als verfügbar in der Liste angezeigt werden, ist davon abhängig, welche Anfälligkeiten Sie mithilfe des LANDesk Patch Manager-Dienstes aktualisiert haben. Sie müssen nicht unbedingt ein Produkt mit einer Erkennungsregel verknüpfen. Verknüpfte Produkte fungieren als Filter während des Anfälligkeitsscans. Wenn keine der angegebenen verknüpften Produkt auf dem Client gefunden werden, wird der Anfälligkeitsscan abgebrochen. Werden jedoch keine Produkte angegeben, setzt der Scanner die Dateiprüfung fort.

- **Name:** Enthält den Namen des ausgewählten Produkts.
- **Anbieter:** Enthält den Namen des Lieferanten des ausgewählten Produkts.
- **Version:** Enthält die Versionsnummer des ausgewählten Produkts.

Registerkarte "Dateien"

- **Dateien:** Zeigt die Dateibedingungen an, mit deren Hilfe ermittelt wird, ob die Anfälligkeit auf einem Zielclient existiert. Wählen Sie eine Datei in der Liste aus, um deren Überprüfungsmethode und erwarteten Parameter anzuzeigen. Wenn eine dieser Bedingungen NICHT erfüllt wird, wird konstatiert, dass die Anfälligkeit auf diesem Client existiert. Wenn keine Dateibedingungen in der Liste geführt werden, setzt der Scan die Registrierungsprüfung fort.

  Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie auf **Hinzufügen** klicken, um Felder editierbar zu machen. Auf diese Weise können Sie eine neue Dateibedingung und erwartete Werte/Parameter konfigurieren. Eine Regel kann eine oder mehrere Dateibedingungen einschließen, je nachdem, wie komplex Sie die Regel gestalten möchten. Zum Speichern einer Dateibedingung klicken Sie auf **Aktualisieren**. Zum Löschen einer Dateibedingung aus der Liste wählen Sie die betreffende Bedingung aus und klicken auf **Entfernen**.

- **Überprüfen unter Verwendung von:** Zeigt an, welche Methode zur Überprüfung verwendet werden soll, wenn die angegebene Dateibedingung auf den gescannten Geräten/Clients vorgefunden wird. Beispiel: Eine Erkennungsregel kann auf "Dateiexistenz", "Version", "Datum", "Größe" etc. prüfen. Die erwarteten Parameter, die unterhalb der Prüfmethode angezeigt werden, werden durch die Methode selbst bestimmt (siehe nachstehende Liste).

  Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie die Prüfmethode auswählen, indem Sie auf die Dropdown-Liste **Überprüfen unter Verwendung von** klicken. Wie oben angegeben variieren die Parameterfelder je nach Prüfmethode. Eine Beschreibung der Parameter finden Sie in der nachstehenden Liste.

  - **Nur Dateiexistenz:** Prüft, indem nach der angegebenen Datei gesucht wird. Zulässige Parameter: Pfad (Speicherort der Datei auf der Festplatte (einschließlich Dateiname) und Voraussetzung (muss existieren oder muss nicht existieren).
  - **Dateiversion:** Prüft, indem nach der angegebenen Datei und deren Versionsnummer gesucht wird. Zulässige Parameter: Pfad, Mindestversion und Voraussetzung (muss existieren, muss nicht existieren, kann existieren).

  Hinweis: Für die Parameter "Dateiversion", "Datum" und "Größe" können Sie auf die Schaltfläche **Daten sammeln** klicken, nachdem Sie den Dateipfad und -namen angegeben haben. Auf diese Weise werden die Wertefelder automatisch gefüllt.

  - **Dateidatum:** Prüft, indem nach der angegebenen Datei und deren Datum gesucht wird. Zulässige Parameter: Pfad, Mindestdatum und Voraussetzung (muss existieren, muss nicht existieren, kann existieren).

- **Dateigröße und/oder Prüfsumme:** Prüft, indem nach der angegebenen Datei und deren Größe und Prüfsummenwert gesucht wird. Zulässige Parameter: Pfad, Prüfsumme, Dateigröße und Voraussetzung (muss existieren, muss nicht existieren, kann existieren).
- **MSI Produkt-ID installiert:** Führt einen Scan durch, um sicherzustellen, dass das MSI-Produkt installiert ist (ein von Microsoft Installer installiertes Produkt). Zulässige Parameter: Guid (die globale eindeutige Produktkennung).
- **MSI Produkt-ID NICHT installiert:** Führt einen Scan durch, um sicherzustellen, dass das angegebene MSI-Produtk nicht installiert ist. Zulässige Parameter: Guid.

Register "Registrierung"

- **Registrierung:** Zeigt die Registrierungsbedingungen an, mit deren Hilfe ermittelt wird, ob die Anfälligkeit auf einem Zielclient existiert. Wählen Sie einen Registrierungsschlüssel in der Liste aus, um dessen erwartete Parameter anzuzeigen. Wenn eine dieser Bedingungen NICHT erfüllt wird, wird konstatiert, dass die Anfälligkeit auf diesem Client existiert. Wenn keine Registrierungsbedingungen in der Liste aufgeführt werden UND keine Dateibedingungen auf der Registerkarte "Dateien" angegeben waren, misslingt der Scan. Mit anderen Worten - eine Erkennungsregel muss mindestens eine Datei- oder Registrierungsbedingung enthalten.

  Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie auf **Hinzufügen** klicken, um Felder editierbar zu machen. Auf diese Weise können Sie eine neue Bedingung für den Registrierungsschlüssel und erwartete Parameter konfigurieren. Eine Regel kann eine oder mehrere Registrierungsbedingungen umfassen. Zum Speichern einer Registrierungsbedingung klicken Sie auf **Aktualisieren**. Um eine Registrierungsbedingung aus der Liste zu löschen, wählen Sie die betreffende Bedingung aus und klicken auf **Entfernen**.

- **Schlüssel:** Benennt den erwarteten Ordner und Pfad des Registrierungsschlüssels.
- **Name:** Benennt den erwarteten Namen des Schlüssels.
- **Wert:** Benennt den erwarteten Wert des Schlüssels.
- **Erforderlich:** Zeigt an, ob der Registrierungsschlüssel auf Zielgeräten existieren muss oder nicht.

Registerkarte "Kommentare"

- **Kommentare:** Zeigt zusätzliche Informationen über den Patch-Anbieter an, falls verfügbar. Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie nach Bedarf eigene Kommentare eingeben.

Registerkarte "Befehle"

Die Registerkarte "Befehle" wird NUR angezeigt, wenn die Anfälligkeit benutzerdefiniert ist und die ausgewählte Erkennungsregel eine Sanierung durchführt. Diese Registerkarte wird bei Anfälligkeiten, die über den Patch Manager heruntergeladen werden, oder bei benutzerdefinierten Anfälligkeiten, die nur einen Erkennungsvorgang ausführen, nicht eingeblendet.

Verwenden Sie diese Registerkarte zum Konfigurieren von Zusatzbefehlen, die als Teil des Reparaturvorgangs ausgeführt werden. Diese Befehle sind nützlich, wenn Sie konkrete Aktionen auf Zielclients programmieren müssen, um eine erfolgreiche Reparatur zu gewährleisten. Zusätzliche Befehle sind nicht erforderlich. Wenn Sie keine zusätzlichen Befehle konfigurieren, wird die Patchdatei standardmäßig für sich allein ausgeführt. Wenn Sie dagegen einen oder mehrere zusätzliche Befehle konfigurieren, müssen Sie die Patchdatei mit dem Befehl "Ausführen" ausführen.

- **Befehle:** Zeigt Befehle in der Reihenfolge ihrer Ausführung auf Zielclients an. Wählen Sie einen Befehl aus, um seine Argumente anzuzeigen. Sie können die Befehlsreihenfolge mithilfe der Schaltflächen **Nach oben** und **Nach unten** ändern. Um einen Befehl aus der Liste zu entfernen, wählen Sie ihn aus und klicken auf **Entfernen**.
- **Hinzufügen:**Öffnet ein Dialogfeld, in dem Sie einen Befehlstyp für die Liste "Befehle" auswählen können.
- **Befehlsargumente:**Zeigt die Argumente an, die den ausgewählten Befehl definieren. Die Werte eines Arguments können bearbeitet werden. Sie können ein Argument bearbeiten, indem Sie auf das Feld **Wert** dieses Arguments doppelklicken und dann direkt in das Feld Werte eingeben. Bei allen Befehlstypen können Sie auch mit der rechten Maustaste in das Feld **Wert** klicken, um einen Makro/eine Variable in das Argument einzufügen.

  Die folgende Liste beschreibt die Befehle und ihre Argumente:

- **Kopierbefehl:**Kopiert eine Datei aus der angegebenen Quelle in das angegebene Ziel auf den Festplatten der Clients. Diese Befehle können vor und/oder nach der Ausführung des tatsächlichen Patch ausgeführt werden. Beispiel: Nachdem Sie den Inhalt einer komprimierten Datei mit dem Unzip-Befehl extrahiert haben, möchten Sie Dateien von einem Speicherort in einen anderen kopieren.

  Die Argumente für den Kopierbefehl lauten: Ziel (Pfad, in den Sie die Datei kopieren möchten, ausschließlich des Dateinamens) und Quelle(vollständiger Pfad und Dateiname der Datei, die Sie kopieren möchten).

- **Ausführen:**Führt die Patchdatei oder jede andere ausführbare Datei auf den Zielclients aus.

Die Argumente für den Aufführungsbefehl lauten: Pfad (vollständiger Pfad und Dateiname des Speicherortes, an dem sich die ausführbare Datei befindet; für die Patchdatei können Sie die Variablen %SDMCACHE% und %PATCHFILENAME% verwenden), Args (Befehlszeilenoptionen für die ausführbare Datei; beachten Sie, dass dieses Feld kein erforderliches Feld ist), Timeout (Anzahl von Sekunden, die bis zur vollständigen Ausführung der ausführbaren Datei abgewartet werden soll, bevor der Vorgang mit dem nächsten Befehl in der Liste fortgesetzt wird - gilt, wenn für das Argument "Wait" die Einstellung "Wahr" gewählt wurde) und Wait ("Wahr"- oder "Falsch"-Wert, der festlegt, ob die vollständige Ausführung der ausführbaren Datei abgewartet werden soll, bevor der Vorgang mit dem nächsten Befehl in der Liste fortgesetzt wird).

- **ButtonClick:**Klickt automatisch auf eine angegebene Schaltfläche, die während der Ausführung einer ausführbaren Datei angezeigt wird. Mit diesem Befehl können Sie einen Schaltflächen-Mausklick programmieren, sofern eine solche Interaktion von der ausführbaren Datei verlangt wird.

  Damit "ButtonClick" ordnungsgemäß funktioniert, muss das Argument "Wait" für den vorhergehenden Ausführungsbefehl auf "falsch" gesetzt werden. Mit dieser Vorgehensweise stellen Sie sicher, dass die ausführbare Datei vor dem Weitermachen mit der Klick-Aktion auf die Schaltfläche nicht beendet werden muss.

  Die Argumente für den ButtonClick-Befehl lauten: Erforderlich (der Wert "wahr" oder "falsch" gibt an, ob die Schaltfläche angeklickt werden muss, damit der Vorgang fortgesetzt werden kann; wenn Sie "wahr" auswählen und die Schaltfläche sich aus irgendeinem Grund nicht anklicken lässt, wird die Reparatur fortgesetzt), ButtonIDorCaption (benennt die anzuklickende Schaltfläche anhand ihres Text-Labels oder ihrer Control-ID), Timeout (Anzahl von Sekunden, die die anzuklickende Schaltfläche während der Ausführung der ausführbaren Datei eingeblendet wird) und WindowCaption (benennt das Fenster oder Dialogfeld, in dem sich die anzuklickende Schaltfläche befindet).

- **ReplaceInFile:**Bearbeitet eine textbasierte Datei auf Zielclients. Verwenden Sie diesen Befehl, wenn Sie vor oder nach dem Ausführen der Patchdatei Änderungen in einer textbasierten Datei vornehmen müssen (beispielsweise Änderung eines bestimmten Wertes in einer .INI-Datei), um sicherzustellen, dass die Datei korrekt ausgeführt wird.

  Die Argumente für den ReplaceInFile-Befehl lauten: Dateiname (vollständiger Pfad und Name der Datei, die Sie bearbeiten möchten), ReplaceWith (exakte Textzeichenfolge, die Sie zur Datei hinzufügen möchten) und Original Text (exakte Textzeichenfolge, die Sie in der Datei ersetzen möchten).

- **StartService:**Startet einen Dienst auf Zielclients. Verwenden Sie diesen Befehl, um einen Dienst zu starten, der benötigt wird, um die Patchdatei ausführen zu können, oder um einen Dienst neu zu starten, der zuvor gestoppt werden musste, damit die Patchdatei ausgeführt werden konnte.

  Die Argumente für den StartService-Befehl lauten: Dienst (Name des Dienstes).

- **StopService:**Stoppt einen Dienst auf Zielclients. Verwenden Sie diesen Befehl, wenn ein Dienst auf einem Client gestoppt werden muss, damit die Patchdatei installiert werden kann.

  Die Argumente für den StopService-Befehl lauten: Dienst (Name des Dienstes).

- **Unzip:**Entzippt eine komprimierte Datei auf Zielclients. Sie können diesen Befehl beispielsweise verwenden, wenn die Reparatur die Ausführung oder das Kopieren mehrerer Dateien auf die Zielclients erforderlich macht.

  Die Argumente für den Unzip-Befehl lauten: Ziel (vollständiger Pfad, in dem Sie den Inhalt einer komprimierten Datei auf der Festplatte eines Clients extrahieren möchten) und Quelle (vollständiger Pfad und Dateiname der komprimierten Datei).

Löschen von Anfälligkeits- und Erkennungsregelinformationen

Sie können Anfälligkeitsinformationen aus dem Patch Manager-Fenster (und der Core-Datenbank) löschen, wenn Sie feststellen, dass diese Informationen für Ihre Umgebung nicht von Belang sind, oder wenn Anfälligkeiten erfolgreich saniert werden konnten und die Informationen daher veraltet sind.

Beim Löschen von Anfälligkeitsinformationen werden auch die zugehörigen Erkennungsregelinformationen aus den Erkennungsregelgruppen in der Baumansicht entfernt. Die eigentlichen ausführbaren Patchdateien werden bei diesem Vorgang jedoch nicht entfernt. Die Patchdateien müssen von Hand aus der lokalen Ablage gelöscht werden, die sich in der Regel auf dem Core Server befindet.

So löschen Sie Anfälligkeitsinformationen

1. Klicken Sie auf **Extras | Patch Manager**.
2. Klicken Sie auf die Schaltfläche **Nicht verwendete Anfälligkeiten entfernen** in der Symbolleiste.
3. Wählen Sie die Plattformen aus, deren Anfälligkeitsinformationen entfernt werden sollen. Sie können eine oder mehrere Plattformen aus der Liste wählen.

   Falls eine Anfälligkeit mit mehreren Plattformen verbunden ist, müssen Sie alle zugehörigen Plattformen auswählen, damit die Anfälligkeitsinformationen entfernt werden können.

4. Wählen Sie die Sprachen aus, deren Anfälligkeitsinformationen entfernt werden sollen (in Verbindung mit der oben ausgewählten Plattform).

   Wenn Sie oben eine Windows-Plattform auswählen, müssen Sie angeben, für welche Sprache die Anfälligkeitsinformationen entfernt werden sollen. Haben Sie oben eine UNIX-Plattform ausgewählt, dann müssen Sie die Option "Sprache neutral" angeben, damit die sprachübergreifenden Anfälligkeitsinformationen entfernt werden. Weitere Informationen zu den Sprachoptionen finden Sie unter "Übersicht über die Option "Sprache neutral"" weiter oben in diesem Kapitel.

5. Klicken Sie auf **Entfernen**.

Informationen zum Dialogfeld "Nicht verwendete Anfälligkeitsinformationen entfernen"

Verwenden Sie dieses Dialogfeld zum Entfernen von Informationen zu Anfälligkeiten und den damit verbundenen Patches zu entfernen.

- **Plattformen zum Entfernen auswählen:** Legt fest, zu welcher Plattform Anfälligkeitsinformationen aus der Core-Datenbank gelöscht werden.
- **Sprachen zum Entfernen auswählen:** Legt die Sprachversion der Anfälligkeiten der ausgewählten Plattform fest, deren Informationen entfernt werden. Siehe oben Schritt 4.
- **Entfernen:** Entfernt die Anfälligkeits- und Erkennungsregelinformationen für die ausgewählte(n) Plattform(en) und Sprache(n).
- **Schließen:** Schließt das Dialogfeld, wobei weder Änderungen gespeichert noch Anfälligkeitsinformationen gelöscht werden.

Scannen von Clients auf Anfälligkeiten

Eine Anfälligkeitsbewertung bedeutet, dass die auf einem Client aktuell installierten Versionen von Betriebssystemdateien und anwendungsspezifischen Dateien sowie die Registrierungsschlüssel auf die neuesten bekannten Anfälligkeiten überprüft werden, um Sicherheitsrisiken in einem System zu identifizieren.

Nachdem Sie die Informationen zu bekannten Anfälligkeiten (aktualisiert mit Informationen aus den relevanten Quellen der IT-Industrie) überprüft und entschieden haben, nach welchen Anfälligkeiten gescannt werden soll, können Sie auf verwalteten Clients, auf denen der Anfälligkeitsscanner-Agent installiert ist, eine benutzerdefinierte Anfälligkeitsbewertung durchführen. (Weitere Informationen zum Konfigurieren von Clients für das Anfälligkeitsscanning und die Patchverteilung finden Sie unter Konfigurieren von Clients für den Patch Manager" weiter oben in diesem Kapitel).

Sie können selbstverständlich auch jederzeit Ihre eigenen benutzerdefinierten Anfälligkeiten für Anfälligkeitsscans verwenden.

Wenn der Anfälligkeitsscanner ausgeführt wird, liest er stets die Einträge der Gruppe "Aktivierte Anfälligkeiten" und sucht nach diesen speziellen Anfälligkeiten. Bevor Sie ein Gerät (oder mehrere Geräte) auf Anfälligkeiten überprüfen, sollten Sie daher immer sicherstellen, dass die entsprechenden Anfälligkeiten in dieser Gruppe enthalten sind. Sie können Anfälligkeiten jederzeit manuell in die Gruppe "Aktivierte Anfälligkeiten" verschieben oder daraus entfernen. Überdies können Sie einen Prozess zur Aktualisierung von Anfälligkeiten konfigurieren, sodass automatisch neue Anfälligkeiten der Gruppe "Aktivierte Anfälligkeiten" hinzugefügt werden.

Wie bereits angemerkt, wird der Anfälligkeitsscanner zum ersten Mal automatisch im Rahmen der Clientkonfiguration auf den Zielclients ausgeführt, wenn der Anfälligkeitsscanner-Agent in einem Clientkonfigurationsskript zur Installation ausgewählt wird.

Der Anfälligkeitsscanner fügt die Anfälligkeitsinformationen den Inventardaten des Clients in der Core-Datenbank hinzu. Diese Informationen können zur Erzeugung von anfälligkeitsspezifischen Abfragen, Richtlinien und Berichten verwendet werden. Um die Anfälligkeitsinformationen zu einem Client anzuzeigen, klicken Sie mit der rechten Maustaste auf den betreffenden Client und klicken dann auf **Anfälligkeitsinformationen**.

Vorsicht beim Entfernen von Anfälligkeiten aus der Gruppe "Aktivierte Anfälligkeiten"
Wenn Sie Anfälligkeiten von der Gruppe "Aktivierte Anfälligkeiten" in die Gruppe "Deaktivierte Anfälligkeiten" verschieben, dann werden die aktuellen Daten zur Anfälligkeitsbewertung (Daten in der Core-Datenbank, die besagen, auf welchen überprüften Clients diese Anfälligkeiten erkannt wurden) aus der Core-Datenbank entfernt und sind weder in den Eigenschaftsdialogfeldern der betreffenden Anfälligkeiten noch in den Dialogfeldern "Anfälligkeitsinformationen" auf den betreffenden Clients verfügbar. Um diese Anfälligkeitsbewertungsdaten wiederherzustellen, müssten Sie die Anfälligkeiten wieder in die Gruppe "Aktivierte Anfälligkeiten" schieben und einen neuen Anfälligkeitsscan durchführen.

Der Anfälligkeitsscanner kann auf einem Client direkt aufgerufen werden (klicken Sie auf **Start | Programme | LANDesk Management | Anfälligkeitsscanner**) oder vom Core Server als Task vom Typ "Auf Anfälligkeiten prüfen" mittels Push auf Clients gestartet werden.

So prüfen Sie im Rahmen eines geplanten Task auf Anfälligkeiten

1. Klicken Sie auf **Extras | Patch Manager**.
2. Stellen Sie sicher, dass die Anfälligkeitsinformationen kürzlich aktualisiert worden sind.
3. Stellen Sie sicher, dass die Gruppe "Aktivierte Anfälligkeiten" nur diejenigen Anfälligkeiten enthält, auf die Sie prüfen möchten.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anfälligkeitsscan planen**, um den Task dem Fenster "Geplante Tasks" hinzuzufügen.
5. Fügen Sie die Zielclients hinzu, die überprüft werden sollen.
6. Klicken Sie in der Symbolleiste auf die Schaltfläche **Startzeit festlegen** und konfigurieren Sie Uhrzeit und Wiederholungsintervall des Task nach Belieben. Weitere Informationen finden Sie im Kapitel über das Konfigurieren von Clients unter "Planen von Tasks".
7. Klicken Sie auf **OK**.

Anfälligkeitsprotokolldatei
Der Anfälligkeitsscanner legt eine Protokolldatei namens **vulscan.log** mit Daten über den aktuellsten Scan auf dem Client an und speichert zudem die letzten fünf Protokolldateien in chronologischer Reihenfolge nach Nummern geordnet. Diese Protokolldateien enthalten Informationen über den Zeitpunkt des Anfälligkeitsscans, die Sprache, die Plattform (wobei Windows 95/98 durch Win9x, Windows 2000 durch Win2k und Windows XP/2003 durch WinXP dargestellt wird) und die Prozesse, die vom Scanner ausgeführt wurden.

Anzeigen des Datums des letzten Anfälligkeitsscans

Sie können feststellen, wann der letzte Anfälligkeitsscan auf einem Gerät durchgeführt wurde, indem Sie mit der rechten Maustaste auf das Gerät klicken, dann auf **Inventar** klicken und nach unten zum Attribut **Datum des letzten Anfälligkeitsscans** blättern, das im rechten Fensterausschnitt der Ansicht "Inventar" angezeigt wird.

Anzeigen erkannter Anfälligkeiten

Wenn der Anfälligkeitsscanner auf irgendeinem Zielgerät irgendeine der aktivierten Anfälligkeiten findet, dann wird diese Information an den Core Server weitergegeben. Sie können nach der Durchführung eines Anfälligkeitsscans unter Verwendung einer der folgenden Methoden erkannte Anfälligkeiten betrachten:

Nach der Gruppe "Erkannte Anfälligkeiten"
Wählen Sie die Gruppe **Erkannte Anfälligkeiten** im Patch Manager-Fenster aus, um eine vollständige Liste sämtlicher Anfälligkeiten anzuzeigen, die während des letzten Anfälligkeitsscans erkannt wurden. In der Spalte "Gescannt" wird angezeigt, wie viele Geräte auf eine Anfälligkeit überprüft wurden, und aus der Spalte "Erkannt" geht hervor, wie viele dieser Geräte von dieser Anfälligkeit betroffen sind.

Nach einer Anfälligkeit
Klicken Sie mit der rechten Maustaste auf eine Anfälligkeit und klicken Sie dann auf **Betroffene Computer**, um eine Liste der Geräte anzuzeigen, auf denen die Anfälligkeit während des letzten Anfälligkeitsscans festgestellt wurde.

Nach einem einzelnen Gerät
Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf ein bestimmtes Gerät und klicken Sie dann auf **Anfälligkeitsinformationen**, um detaillierte Angaben zur Anfälligkeitsbewertung und dem Status der Patchverteilung für dieses Gerät anzuzeigen (siehe "Informationen zum Dialogfeld "Anfälligkeitsinformationen"").

Nach einer Gruppe ausgewählter Geräte
Wählen Sie in der Netzwerkansicht mehrere Geräte aus, klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie dann **Anfälligkeitsinformationen**, um eine Liste der Anfälligkeiten anzuzeigen, die auf einem oder mehreren dieser Geräte erkannt wurden. Wenn Sie eine Anfälligkeit in dieser Liste auswählen, dann werden im unteren Fensterausschnitt diejenigen Geräte angezeigt, auf denen die betreffende Anfälligkeit während des letzten Anfälligkeitsscans erkannt wurde.

Informationen zum Dialogfeld "Anfälligkeitsinformationen"

Sie verwenden dieses Dialogfeld, um detaillierte Angaben zur Anfälligkeitsbewertung und zum Status der Patchverteilung für ein Gerät anzuzeigen. Sie können in dieser Ansicht auch mit der rechten Maustaste auf eine Anfälligkeit klicken und sofort einen Reparaturauftrag erstellen oder die Funktion "Automatisches Korrigieren" aktivieren oder deaktivieren.

- **Anfälligkeiten erkannt:** Wählen Sie diese Option aus, um sämtliche Anfälligkeiten des Geräts anzuzeigen, die während des letzten Scans erkannt wurden.
- **Nicht erkannte Anfälligkeiten:** Wählen Sie diese Option aus, um die Anfälligkeiten anzuzeigen, die in den letzten Scan einbezogen waren, auf dem Gerät aber nicht erkannt wurden.
- **Anfälligkeitsinformationen:**
    - **Anfälligkeit:** Zeigt den Titel der ausgewählten Anfälligkeit an.
    - **Erkannt:** Gibt an, ob die ausgewählte Anfälligkeit erkannt wurde.

  - **Zuerst erkannt:** Zeigt das Datum und die Uhrzeit an, zu der die Anfälligkeit zum ersten Mal auf dem Gerät erkannt wurde. Diese Informationen können nützlich sein, wenn Sie mehrere Scans ausgeführt haben.
  - **Grund:** Beschreibt den Grund für die Erkennung der ausgewählten Anfälligkeit. Diese Information kann hilfreich sein bei der Entscheidung, ob die Anfälligkeit ein so ernstes Sicherheitsrisiko darstellt, dass sofort Abhilfe geschaffen werden muss.
  - **Erwartet:** Zeigt die Versionsnummer der Datei oder des Registrierungsschlüssels an, nach dem der Anfälligkeitsscanner sucht. Falls die Versionsnummer der Datei oder des Registrierungsschlüssels auf dem gescannten Gerät dieser Nummer entspricht, dann ist keine Anfälligkeit gegeben.
  - **Gefunden:** Zeigt die Versionsnummer der Datei oder des Registrierungsschlüssels an, die auf dem gescannten Gerät festgestellt wurde. Falls sich diese Nummer von der oben erwarteten Nummer unterscheidet, ist eine Anfälligkeit gegeben.
- **Patchinformationen:**
  - **Patch erforderlich:** Zeigt den Dateinamen des ausführbaren Patches an, der zur Behebung der ausgewählten Anfälligkeit erforderlich ist.
  - **Installationsdatum:** Zeigt Datum und Uhrzeit der Patchinstallation auf dem Gerät an, sofern zutreffend.
  - **Installationsstatus:** Gibt an, ob die Verteilung/Installation erfolgreich ausgeführt wurde. Falls die Installation fehlschlug, müssen Sie diese Statusinformation löschen, bevor Sie den Patch erneut zu installieren versuchen.
  - **Patchinstallationsstatus löschen:** Löscht das aktuelle Patch-Installationsdatum und den aktuellen Patchstatus für den ausgewählten Client. Diese Informationen müssen gelöscht werden, um eine erneuten Verteilungs- und Installationsversuch mit dem Patch durchführen zu können.

Herunterladen von Patches

Damit Sicherheits-Patches an anfällige Geräte verteilt werden können, MUSS die ausführbare Datei des Patches auf eine lokale Patchablage im lokalen Netzwerk heruntergeladen werden. Als Standardspeicherort für Patchdownloads ist das Verzeichnis /LDLogon/Patches auf dem Core Server vorgegeben. Sie können diesen Speicherort auf der Registerkarte "Patch" des Dialogfelds "Anfälligkeitseinstellungen aktualisieren" ändern.

Einstellungen zu Speicherort und Proxy-Server für Patchdownloads
Bei Patchdownloads werden immer die aktuellen Einstellungen für den Download-Speicherort aus der Registerkarte "Patch" des Dialogfelds "Anfälligkeitseinstellungen aktualisieren" verwendet. Beachten Sie zudem, dass Sie zuerst die Einstellungen für den Proxy-Server auf der Registerkarte "Proxy-Server" des Dialogfelds "Anfälligkeitseinstellungen aktualisieren" entsprechend konfigurieren müssen, falls Ihr Netzwerk einen Proxy-Server für den Internet-Zugang verwendet, bevor Sie Patchdateien herunterladen können.

Patch Manager versucht zuerst, Patchdateien von der im Dialogfeld "Patcheigenschaften" angezeigten URL herunterzuladen. Falls keine Verbindung hergestellt werden kann oder der Patch aus irgendeinem Grund nicht verfügbar ist, lädt Patch Manager den Patch vom LANDesk Patch Manager-Dienst herunter, d. h. aus einer von LANDesk bereitgestellten Datenbank, die Patches aus Quellen der IT-Branche enthält.

Sie können jeden Patch einzeln oder mehrere Patches gleichzeitig herunterladen.

So laden Sie Patches herunter

1. Klicken Sie in einer beliebigen Erkennungsregelgruppe im Patch Manager-Fenster mit der rechten Maustaste auf eine Erkennungsregel und klicken Sie dann auf **Patch herunterladen**. Sie können auch Patches für benutzerdefinierte Anfälligkeiten aus dem Dialogfeld "Erkennungsregel" herunterladen, wenn Sie eine benutzerdefinierte Anfälligkeit erstellen oder bearbeiten.
2. Um eine Gruppe von Patches herunterzuladen, wählen Sie eine beliebige Anzahl von Regeln in einer der Erkennungsregelgruppen aus, klicken mit der rechten Maustaste auf die Auswahl und klicken dann auf **Download**.
3. Informationen zum Download-Vorgang und –Status werden im Dialogfeld "Patches werden heruntergeladen" angezeigt. Sie können jederzeit auf **Abbrechen** klicken, um den gesamten Download-Vorgang zu stoppen.
4. Wenn der Download beendet ist, klicken Sie auf die Schaltfläche **Schließen**.

Weitere Informationen zum Patchdatei-Download-Status finden Sie unter "Informationen zum Patch Manager-Fenster" weiter oben in diesem Kapitel.

Entfernen von Patchdateien

Um Patchdateien zu entfernen, müssen Sie die Dateien von Hand aus der Patchablage löschen, die sich für gewöhnlich auf dem Core Server befindet.

Reparieren von Anfälligkeiten

Nachdem Sie die Anfälligkeiten aktualisiert oder eigene benutzerdefinierte Anfälligkeiten erstellt, Clients überprüft, kritische Anfälligkeiten ermittelt und Patches heruntergeladen haben, besteht der nächste Schritt zur Implementierung der Patchverwaltung darin, Anfälligkeiten durch die Verteilung und Installation der notwendigen Patches auf Zielclients zu reparieren.

Beachten Sie, dass das Beheben von Anfälligkeiten, ähnlich wie das Prüfen auf Anfälligkeiten, nur auf Clients funktioniert, die mit dem Anfälligkeitsscanner-Agenten konfiguriert worden sind. Weitere Informationen hierzu finden Sie unter "Konfigurieren von Clients für den Patch Manager" weiter oben in diesem Kapitel.

Patch Manager installiert nur diejenigen Patches, die auf einem bestimmten Gerät erforderlich sind, und nicht sämtliche Patches, die für die im Reparaturauftrag enthaltenen Anfälligkeiten relevant sind.

Patch Manager kann auch die fortgeschrittenen Paketverteilungsfunktionen von Management Suite nutzen, um Patches schnell und effizient zu verteilen; zu diesen Funktionen zählen Targeted Multicast, Peerdownload und Checkpoint-Neustart. Weitere Informationen zu diesen Funktionen finden Sie im Kapitel "Verteilen von Software und Dateien".

Manuelles Reparieren von Mac- und UNIX-Clients
Unterstützte Windows-Clients können mit jeder der hier beschriebenen Methoden von der Management Suite-Konsole aus behandelt werden; dagegen können andere unterstützte Clients wie Mac OS X und UNIX Sun Solaris von der Management Suite-Konsole aus nur gescannt, aber nicht behandelt werden. Sowohl auf Mac- als auch auf UNIX-Clients müssen Patches von Hand installiert werden.

Einzel- und Gruppenbehandlung

Mit jeder der im Folgenden beschriebenen drei Behandlungsmethoden können Sie eine einzelne Anfälligkeit oder eine Gruppe von Anfälligkeiten reparieren.

Um einzelne Anfälligkeiten nacheinander zu behandeln, klicken Sie mit der rechten Maustaste auf eine Anfälligkeit und wählen dann **Reparieren**.

Um eine Gruppe von Anfälligkeiten gemeinsam zu behandeln, kopieren Sie die Anfälligkeiten aus einer der Anfälligkeitsgruppen in eine benutzerdefinierte Gruppe (siehe "Informationen zum Patch Manager-Fenster" weiter oben in diesem Kapitel), klicken mit der rechten Maustaste auf die Gruppe und klicken dann auf **Reparieren**. Die Funktion "Automatisches Korrigieren" ist für benutzerdefinierte Gruppen allerdings nicht verfügbar. Sie können jedoch mehrere Anfälligkeiten in einer Liste auswählen, mit der rechten Maustaste darauf klicken und **Automatisches Korrigieren** wählen.

Behandlungsmethoden

LANDesk Patch Manager stellt die folgenden Methoden zum Beheben von Anfälligkeiten (sowohl für einzelne Anfälligkeiten als ach für Gruppen von Anfälligkeiten) zur Verfügung:

- Geplanter Task
- Richtlinienbasiert
- Automatisches Korrigieren

Die Behandlung mittels eines geplanten Task kann mit einer Push-Verteilung verglichen werden, weil der Patch vom Core Server mittels Push an die Zielclients übermittelt wird. Eine Richtlinie wird dagegen als Pull-Verteilung betrachtet, weil der Richtlinienagent des Clients auf dem Core Server nach zutreffenden Richtlinien sucht und den Patch dann mittels Pull vom Core Server abruft.

Behandlung mithilfe eines geplanten Task

Eine Behandlung mithilfe eines geplanten Task ist sinnvoll, wenn ein Reparaturauftrag zu einem bestimmten späteren Zeitpunkt oder als wiederkehrende Aufgabe ausgeführt werden soll. Patch Manager verwendet das Tool "Geplante Tasks", um einen geplanten Task zur Behebung einer Anfälligkeit zu konfigurieren und zu bearbeiten.

So konfigurieren Sie eine Behandlung mithilfe eines geplanten Task

1. Klicken Sie auf **Extras | Patch Manager**.
2. Klicken Sie mit der rechten Maustaste auf eine Anfälligkeit in einer der Anfälligkeitsgruppen, oder klicken Sie mit der rechten Maustaste auf eine benutzerdefinierte Anfälligkeitsgruppe.
3. Klicken Sie auf **Reparieren**.
4. Bearbeiten Sie den Eintrag im Feld "Auftragsname", wenn Sie den Namen des Reparaturauftrags ändern möchten.
5. Markieren Sie das Kontrollkästchen **Als geplanten Task reparieren**.
6. (Optional) Wenn die aktuell anfälligen Clients automatisch der Zielliste im Fenster "Geplante Tasks" hinzugefügt werden sollen, markieren Sie das Kontrollkästchen **Der Zielliste für den Task anfällige Knoten hinzufügen**. Mit anfälligen Clients sind diejenigen Geräte gemeint, auf denen die Anfälligkeit während des letzten Anfälligkeitsscans erkannt wurde. Sobald der Task im Fenster "Geplante Tasks" erstellt wurde, können Sie weitere Ziele hinzufügen.
7. (Optional) Falls die Patches mittels Targeted Multicast verteilt werden sollen, markieren Sie das Kontrollkästchen **Multicast verwenden**. Zum Konfigurieren der Multicast-Optionen klicken Sie auf die Schaltfläche **Multicast-Optionen**. Weitere Informationen finden Sie unter "Info über die Seite "Multicast-Optionen"".
8. (Optional) Wenn Sie Peerdownload nur für die Patchverteilung verwenden möchten, aktivieren Sie das Kontrollkästchen **Peerdownload**. Wenn diese Option ausgewählt ist, wird die Patchdatei nur verteilt, wenn sie sich entweder im lokalen Cache des Clients befindet oder in einem Peer in demselben Subnetz. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Patchinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn er sich an einem dieser beiden Orte befindet.

9. (Optional) Wenn Sie sicherstellen möchten, dass Zielclients nicht automatisch neu starten, unabhängig von den angewendeten Patches, aktivieren Sie das Kontrollkästchen **Nie**. Für manche Patches ist ein Neustart erforderlich. Wenn Sie jedoch diese Option aktivieren, können Sie einen Patch entfernt anwenden und dabei einen automatischen Neustart für die Fälle verhindern, in denen Sie vielleicht den Computer zu einer späteren, passenderen Zeit neu starten möchten.
10. Klicken Sie auf **OK**.
11. Der Task wird im Fenster "Geplante Tasks" unter dem oben angegebenen Auftragsnamen angezeigt; Sie können diesem Auftrag weitere Zielgeräte hinzufügen und Planungsoptionen für den Auftrag konfigurieren.

Richtlinienbasierte Behandlung

Eine richtlinienbasierte Behandlung bietet Flexibilität, da Sie Zielclients basierend auf den Ergebnissen einer benutzerdefinierten LDAP- oder Core-Datenbankabfrage dynamisch festlegen können. Sie können beispielsweise eine Behandlungsrichtlinie so konfigurieren, dass die Behandlung lediglich an Clients aus einem bestimmten Verzeichnis-Container oder nur an Clients mit einem bestimmten Betriebssystem (oder einem anderen abfragbaren Inventarattribut) durchgeführt wird. Patch Manager verwendet Application Policy Management-Tool zum Konfigurieren und Verarbeiten von Behandlungsrichtlinien.

Damit ein Client über eine Richtlinie behandelt werden kann, muss der Application Policy Management-Agent darauf installiert sein. Wenn der Application Policy Management-Agent auf einem Client ausgeführt wird, dann überprüft er, ob in der Core-Datenbank auf den Client anzuwendende Richtlinien vorliegen. Sind solche Richtlinien vorhanden, wird auf dem Client ein Dialogfeld mit empfohlenen und optionalen Richtlinien (erforderliche Richtlinien, die automatisch angewendet werden) angezeigt.

Behandlungs- (oder Reparatur-) richtlinien funktionieren ganz ähnlich wie Anwendungsrichtlinien, abgesehen davon, dass Patchdateien statt Anwendungsdateien verteilt werden. Für Reparatur- und Anwendungsrichtlinien gelten im Grunde dieselben Voraussetzungen für die Richtlinienverwaltung, dieselben Bedingungen für den Taskfluss, dieselben Richtlinientypen und dieselben Bedingungen für die statische und dynamische Auswahl der Zielclients. Weitere Informationen zur Richtlinienverwaltung finden Sie im Kapitel "Verwalten von Anwendungsrichtlinien".

So konfigurieren Sie eine richtlinienbasierte Behandlung

1. Klicken Sie auf **Extras | Patch Manager**.
2. Klicken Sie mit der rechten Maustaste auf eine Anfälligkeit in einer der Anfälligkeitsgruppen, oder klicken Sie mit der rechten Maustaste auf eine benutzerdefinierte Anfälligkeitsgruppe.
3. Klicken Sie auf **Reparieren**.
4. Bearbeiten Sie den Eintrag im Feld "Auftragsname", wenn Sie den Namen des Reparaturauftrags ändern möchten.
5. Markieren Sie das Kontrollkästchen **Als Richtlinie reparieren**.
6. Wenn Sie basierend auf dieser Anfälligkeitsdefinition eine neue Abfrage erstellen möchten, mit der später andere verwaltete Geräte gescannt werden können, aktivieren Sie das Textfeld **Abfrage hinzufügen**.

7. (Optional) Wenn Sie Peerdownload nur für die Patchverteilung verwenden möchten, aktivieren Sie das Kontrollkästchen **Peerdownload**. Wenn diese Option ausgewählt ist, wird die Patchdatei nur verteilt, wenn sie sich entweder im lokalen Cache des Clients befindet oder in einem Peer in demselben Subnetz. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Patchinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn er sich an einem dieser beiden Orte befindet.
8. (Optional) Wenn Sie sicherstellen möchten, dass Zielclients nicht automatisch neu starten, unabhängig von den angewendeten Patches, aktivieren Sie das Kontrollkästchen **Nie**. Für manche Patches ist ein Neustart erforderlich. Wenn Sie jedoch diese Option aktivieren, können Sie einen Patch entfernt anwenden und dabei einen automatischen Neustart für die Fälle verhindern, in denen Sie vielleicht den Computer zu einer späteren, passenderen Zeit neu starten möchten.
9. Klicken Sie auf **OK**.
10. Die neue Richtlinie wird im Application Policy Management-Fenster unter dem oben angegebenen Auftragsnamen angezeigt. Hier können Sie jetzt statische Ziele (Benutzer oder Geräte) und dynamische Ziele (Abfrageergebnisse) hinzufügen sowie Typ und Häufigkeit der Richtlinie konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von Richtlinien" im Kapitel "Verwalten von Anwendungsrichtlinien".

Behandlung durch die Funktion "Automatisches Korrigieren"

"Automatisches Korrigieren" ist eine komfortable, integrierte Funktion zur raschen Behandlung von Fällen, in denen Sie keine(n) geplante(n) Task oder Richtlinie zur Ausführung eines Reparaturauftrags erstellen möchten. Wenn beispielsweise eine neue Anfälligkeit bekannt wird, die Sie in einem Schritt suchen und reparieren möchten, dann können Sie hierzu die Funktion "Automatisches Korrigieren" einsetzen.

Voraussetzungen für den Einsatz der Funktion "Automatisches Korrigieren"
Nur Administratoren oder Benutzer, die zur Ausführung von Patch Manager berechtigt sind UND über den Bereich "Standardbereich: Alle Rechner" verfügen, können die Funktion "Automatisches Korrigieren" für Anfälligkeiten aktivieren. Management Suite-Benutzer, die entweder kein LANDesk Administrator sind oder keine Berechtigung zur Ausführung von Patch Manager besitzen, sehen diese Option noch nicht einmal im Kontextmenü einer Anfälligkeit (das durch Anklicken mit der rechten Maustaste geöffnet wird). Weitere Informationen zu Rechten und Bereichen finden Sie unter "Rollenbasierte Administration" in Kapitel 1.

Wenn die Funktion "Automatisches Korrigieren" aktiviert ist, dann verteilt und installiert Patch Manager automatisch den erforderlichen Patch auf allen betroffenen Zielgeräten, sobald der Anfälligkeitsscanner das nächste Mal ausgeführt wird (wobei dessen Aufruf entweder manuell oder mittels eines Task vom Typ "Auf Anfälligkeiten prüfen" erfolgen kann). Wenn die Funktion "Automatisches Korrigieren" aktiviert ist und ein Patch einen Neustart erforderlich macht, wird das Zielgerät immer automatisch neu gestartet.

Sie können die Funktion "Automatisches Korrigieren" für eine einzelne Anfälligkeit oder eine Gruppe von Anfälligkeiten aktivieren.

Aus der Anzeige von "Ja" bzw. "Nein" in der Spalte "Automatisches Korrigieren" einer Anfälligkeitsgruppenliste geht hervor, ob diese Funktion aktiviert ist.

So konfigurieren Sie eine Behandlung durch die Funktion "Automatisches Korrigieren"

1. Klicken Sie auf **Extras | Patch Manager**.
2. Klicken Sie mit der rechten Maustaste auf eine oder mehrere in den Anfälligkeitsgruppen markierte Anfälligkeit(en). (Sie können die Funktion "Automatisches Korrigieren" nicht für eine bestimmte benutzerdefinierte Anfälligkeitsgruppe aktivieren.)
3. Klicken Sie auf **Automatisches Korrigieren aktivieren**.
4. Führen Sie jetzt den Anfälligkeitsscanner auf denjenigen Geräten aus, die überprüft und automatisch behandelt werden sollen.

Was geschieht während der Behandlung auf dem Client

Eine automatische Behandlung umfasst die Verteilung und Installation von Patches auf verwalteten Windows-Clients, wobei jede der drei in den vorhergehenden Abschnitten beschriebenen Methoden eingesetzt werden kann.

Denken Sie stets daran, dass ein Anfälligkeitsreparaturauftrag die Behandlung einer oder mehrerer Anfälligkeit(en) beinhalten kann. Zudem ist zu beachten, dass die Reparatur einer erkannten Anfälligkeit die Installation eines oder mehrerer Patches erfordern kann. Wegen dieser Faktoren kann die Behandlung, abhängig von der Anzahl und dem Typ der erkannten Anfälligkeiten, zur Folge haben, dass auf dem Client nur eine Patchdatei installiert wird oder dass mehrere Patchdateien auf dem Client installiert werden.

Fast alle Patchdateien können unbeaufsichtigt installiert werden, wobei die Installation keinen Benutzereingriff am Client erfordert. Die Installation einiger Windows 9.x-Patches und Patches für andere Sprachen als Englisch erfordern Benutzereingriffe. Ob ein Patch unbeaufsichtigt installiert werden kann, können Sie der Spalte "Unbeaufsichtigte Installation" in Patchlisten der Patch Manager-Ansicht entnehmen. Weitere Informationen hierzu finden Sie unter "Informationen zum Patch Manager-Fenster" weiter oben in diesem Kapitel.

Konsolidierter Neustart
Wenn die Installation einer Patchdatei einen Neustart erfordert (UND die Option "Nie" im Dialogfeld "Anfälligkeit reparieren" aktiviert ist), installiert Patch Manager zuerst ALLE zu dem betreffenden Reparaturauftrag gehörigen Patches auf dem Client und führt dann nur einmal einen Neustart auf dem Client durch.

Zusätzliche Befehle (nur benutzerdefinierte Anfälligkeiten)

Die benutzerdefinierte Anfälligkeitsreparatur kann nach Bedarf zusätzliche Sonderbefehle einschließen, die während der Erstellung einer benutzerdefinierten Erkennungsregel definiert werden. Diese zusätzlichen Befehle werden in der Reihenfolge, die auf der Registerkarte "Befehle" für die betreffende Regel festgelegt wurde und mit den Befehlsargumenten übereinstimmt. Zusätzliche Befehle können bevor, nachdem und während die eigentliche Patchdatei ausgeführt wird, ausgeführt werden.

Informationen zum Dialogfeld "Anfälligkeit reparieren"

Sie verwenden dieses Dialogfeld, um einen Reparaturauftrag zu konfigurieren.

- **Auftragsname:** Bezeichnet den Reparaturauftrag durch einen eindeutigen Namen. Standardmäßig wird der Name der Anfälligkeit oder der benutzerdefinierten Gruppe verwendet. Sie können diesen Namen bei Bedarf bearbeiten.
- **Als geplanten Task reparieren:** Ermöglicht das Konfigurieren einer Behandlung mithilfe eines geplanten Task.
    - **Der Zielliste für den Task anfällige Knoten hinzufügen:** Fügt der Zielliste im Fenster "Geplante Tasks" automatisch anfällige Clients hinzu. Mit anfälligen Clients sind die betroffenen Geräte gemeint, die während des letzten Anfälligkeitsscans erkannt wurden.
    - **Targeted Multicast verwenden:** Aktiviert Targeted Multicast für die Patchverteilung an die Zielgeräte.
    - **Multicast-Optionen:** Öffnet ein eigenes Dialogfeld, in dem Sie verschiedene Multicast-Optionen konfigurieren können. Weitere Informationen hierzu finden Sie unter "Info über die Seite "Multicast-Optionen"".
- **Als Richtlinie reparieren:** Ermöglicht das Konfigurieren einer richtlinienbasierten Behandlung.
- **Eine Abfrage hinzufügen:** Erstellt auf der Basis der ausgewählten Anfälligkeitsdefinition eine neue Abfrage, die Sie zum Scannen anderer Geräte verwenden können.
- **Peerdownload (nur vom Cache oder Peer installieren):** Beschränkt die Patchverteilung derart, dass diese nur dann stattfindet, wenn sich die Patchdatei im lokalen Cache des Clients oder auf einem Peer im gleichen Subnetz befindet. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Patchinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn er sich an einem dieser beiden Orte befindet.
- **Nie neu starten:** Verhindert den automatischen Neustart von Zielclients, auch in den Fällen, in denen ein Patch einen Neustart erfordert. Wenn Sie diese Option aktivieren, können Sie einen Patch entfernt anwenden und dabei einen automatischen Neustart für die Fälle verhindern, in denen Sie vielleicht den Computer zu einer späteren, passenderen Zeit neu starten möchten. Beachten Sie, dass diese Option nicht für die Reparatur durch die Option "Automatisches Korrigieren" gilt.

Hinweis: Weitere Informationen zu den Funktionen Targeted Multicast und Peerdownload finden Sie im Kapitel "Verteilen von Software und Dateien".

Info über die Seite "Multicast-Optionen"

Sie verwenden dieses Dialogfeld, um die folgenden Targeted Multicast-Optionen für eine Behandlung mithilfe eines geplanten Task zu konfigurieren:

- **Multicast-Domänenerkennung:**
    - **Multicast-Domänenerkennung verwenden:** Wählen Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Auftrag durchzuführen. Bei dieser Option werden die Domänenerkennungsergebnisse für die erneute Verwendung nicht gespeichert.

  - **Multicast-Domänenerkennung verwenden und Ergebnisse speichern:** Wählen Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Auftrag durchzuführen und die Ergebnisse für eine künftige Verwendung zu speichern; somit sparen Sie Zeit bei folgenden Multicasts
  - **Ergebnisse der letzten Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option immer dann, wenn Sie durch Targeted Multicast eine Domänenerkennung durchgeführt und die Ergebnisse gespeichert haben.
- **Domänenrepräsentanten zum Reaktivieren von Computern verwenden:** Verwenden Sie diese Option, wenn Sie Computer, die die "Wake On Lan"-Technologie unterstützen, beim Empfang von Multicast reaktivieren möchten.
- **Wartezeit in Sekunden nach Wake on LAN:** Legt fest, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das Wake On LAN-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden. Wenn Computer im Netzwerk länger als 120 Sekunden zum Starten benötigen, sollten Sie diesen Wert erhöhen. Der zulässige Höchstwert liegt bei 3600 Sekunden (eine Stunde).

Mit der nachfolgenden Option können Sie auftragsspezifische Parameter für das Targeted Multicast konfigurieren. Die Standardwerte sind in der Regel für die meisten Multicasts geeignet. Auswirkungen der Optionen:

- **Höchstzahl gleichzeitig arbeitender Multicast-Domänenrepräsentanten:** Die Zahl der Repräsentanten, die aktiv zur selben Zeit einen Multicast durchführen, ist auf diese Anzahl beschränkt.
- **Verarbeitung von Rechnern einschränken, bei denen Multicast fehlschlug:** Wenn ein Client die Datei über Multicast nicht erhält, wird sie aus dem Web oder vom Dateiserver heruntergeladen. Dieser Parameter kann verwendet werden, um die Anzahl der Clients zu beschränken, die die Datei gleichzeitig erhalten. Wenn z.B. die Höchstanzahl von Threads 200 war und die Höchstanzahl der fehlgeschlagenen Multicast-Threads bei 20 lag, würden im Dialogfeld "Benutzerdefinierte Aufträge" nicht mehr als 20 Computer gleichzeitig verarbeitet werden, bei denen Multicast fehlgeschlagen ist. Das Dialogfeld "Benutzerdefinierte Aufträge" verarbeitet bis 200 Clients gleichzeitig, wenn diese erfolgreich den Multicast erhalten haben. Es verarbeiten jedoch nur maximal 20 der 200 Threads Clients, bei denen der Multicast-Task fehlgeschlagen ist. Wenn dieser Wert auf 0 festgelegt ist, führt das Dialogfeld "Benutzerdefinierte Aufträge" den Verteilungsabschnitt des Task für keinen der Computer durch, auf dem das Multicasting fehlgeschlagen ist.
- **Anzahl von Tagen, die die Dateien im Cache des Clients verbleiben:** Die Zeit, die die Datei, für das Multicasting durchgeführt wird, im Cache auf den einzelnen Zielcomputern bleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Anzahl von Tagen, die die Dateien im Cache des Multicast-Domänenrepräsentanten verbleiben:** Die Zeitspanne, über die die Datei, für das Multicasting durchgeführt wird, im Cache auf dem Multicast-Domänenrepräsentanten verbleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Minimale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Mindestwartezeit zwischen dem Senden von Multicast-Paketen.

Dieser Wert wird nur verwendet, wenn der Domänenrepräsentant kein Multicasting einer Datei aus dem eigenen Cache durchführt. Wenn dieser Parameter nicht festgelegt wird, wird die auf dem Subnetz/Domänenrepräsentantencomputer gespeicherte Mindestruhezeit verwendet. Sie können mithilfe dieses Parameters die Bandbreitennutzung im WAN beschränken.

- **Maximale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Höchstwartezeit zwischen dem Senden von Multicast-Paketen. Weitere Informationen finden Sie weiter oben unter "Mindestzahl in Millisekunden zwischen Paketübertragungen".

Überprüfen des Behandlungsstatus

Nachdem die Behandlung auf den Zielclients durchgeführt wurde, gibt Patch Manager Statusinformationen zu jeder Patchinstallation aus. Sie können den Status der Patchinstallation nach Anfälligkeit oder nach Zielclient getrennt überprüfen.

So überprüfen Sie eine Patchinstallation auf einem Client

1. Führen Sie den Anfälligkeitsscanner auf dem Client aus.
2. Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf einen behandelten Client (ein behandeltes Gerät) und klicken Sie dann auf **Anfälligkeitsinformationen**.
3. Klicken Sie im linken Fensterausschnitt auf den Eintrag **Anfälligkeiten erkannt** und wählen Sie dann im rechten Fensterausschnitt eine bestimmte Anfälligkeit aus.
4. Überprüfen Sie die Felder mit Patchinformationen am unteren Fensterrand.

   Das Feld **Installationsstatus** gibt an, ob die Installation erfolgreich war. Folgende Statuswerte sind möglich: "Erfolgreich", "Fehlgeschlagen" und "Fehler beim Herunterladen".

Falls die Patchinstallation misslungen ist, müssen Sie zuerst die den Installationsstatus betreffenden Informationen löschen, bevor Sie erneut versuchen, den Patch zu installieren. Der Installationsstatus (Reparaturstatus) für den ausgewählten Client kann vom Dialogfeld "Anfälligkeitsinformationen" aus geändert werden. Sie können außerdem den Patch-Installationsstatus nach Anfälligkeit löschen (siehe unten).

Löschen des Anfälligkeitsscan- und Reparaturstatus nach Anfälligkeit

Sie können Anfälligkeitsscan- und Reparaturstatusinformationen für alle von einer Anfälligkeit (oder mehreren Anfälligkeiten) betroffenen Geräte mithilfe des Dialogfelds **Abfrage-/Reparaturstatus löschen** löschen. Wenn eine Patchinstallation misslingt, müssen Sie (wie oben beschrieben) zuerst den Installationsstatus (Reparaturstatus) löschen, bevor Sie erneut versuchen, den Patch zu installieren.

Sie können mit diesem Dialogfeld auch Anfälligkeitsscaninformationen für eine oder mehrere Anfälligkeiten aus der Datenbank löschen.

Um den Anfälligkeitsscan- und Reparaturstatus zu löschen, klicken Sie mit der rechten Maustaste auf die Anfälligkeit und wählen **Abfrage-/Reparaturstatus löschen**, wählen die gewünschte Option aus und klicken dann auf **Löschen**.

Verwenden von Patch Manager-Berichten

Wenn Sie das Add-on Patch Manager auf einem Management Suite 8-System installieren, werden dem Werkzeug "Berichte" mehrere auf die Patchverwaltung bezogene Berichte hinzugefügt.

Patch Manager-Berichte stellen verschiedene hilfreiche Statusinformationen zur Anfälligkeitsbewertung und –behandlung (Patchverteilung) von verwalteten Clients in einem Netzwerk zur Verfügung.

Um auf das Werkzeug "Berichte" zugreifen und Berichte erzeugen und anzeigen zu können, muss der Management Suite-Benutzer entweder über die Berechtigung "LANDesk Administrator" (d. h. uneingeschränkte Rechte) oder bestimmte Berechtigungen für das Werkzeug "Berichte" verfügen.

Patch Manager-Berichte

Die folgenden vordefinierten Berichte sind in der Gruppe "Alle Berichte" im Fenster "Berichte" enthalten:

- **Festgestellte Anfälligkeiten pro Computer:** Enthält eine Liste aller Anfälligkeiten, die auf den ausgewählten Geräten erkannt wurden, und das Datum, an dem diese erkannt wurden.
- **Festgestellte Anfälligkeiten pro Speicherort:** Enthält eine Liste aller Anfälligkeiten, die bei den Geräten an den ausgewählten Orten festgestellt wurden.
- **Festgestellte Anfälligkeiten pro Anfälligkeit:** Enthält eine Liste sämtlicher Geräte, bei denen die ausgewählten Anfälligkeiten erkannt wurden, und das Datum, an dem diese festgestellt wurden.
- **Geräte, die nicht auf Anfälligkeiten gescannt wurden:** Enthält eine Liste aller Geräte, für die keine Anfälligkeitsinformationen in der Core-Datenbank verzeichnet sind.
- **Geräte, die nicht repariert werden konnten:** Enthält eine Liste aller bei den ausgewählten Geräten erkannten Anfälligkeiten, für die kein Patch verteilt werden konnte, sowie das Datum des letzten Reparaturversuchs.
- **"Nicht anfällig" und "Nicht repariert":** Enthält eine Liste aller Geräte, bei denen die ausgewählten Anfälligkeiten nicht festgestellt werden konnten und die daher keinen Patch erforderten.
- **Reparierte Anfälligkeiten pro Computer:** Enthält eine Liste der Anfälligkeiten, für die auf dem/den ausgewählt(en) Gerät(en) ein Patch installiert wurde (einschließlich des Datums, an dem der Patch installiert wurde).
- **Reparierte Anfälligkeiten nach Datum:** Enthält eine Liste der Anfälligkeiten, die innerhalb des gewählten Zeitraums auf den einzelnen behandelten Geräten durch Patches repariert wurden.
- **Reparierte Anfälligkeiten nach Standort:** Enthält eine Liste aller Anfälligkeiten, für die auf den Geräten an den ausgewählten Standorten Patches installiert wurden.
- **Reparierte Anfälligkeiten nach Anfälligkeit:** Enthält eine Liste aller Geräte, auf denen Patches für die ausgewählten Anfälligkeiten installiert wurden.

- **Anfälligkeiten nach Zeiteinheit:** Enthält eine Liste aller Anfälligkeiten, die innerhalb des gewählten Zeitraums auf den einzelnen Geräten festgestellt wurden.

Für diese Berichte gelten dieselben Regeln wie für die Berichte in den Gruppen "Alle Softwarelizenzierungsberichte" und "Alle Anlagenberichte". Sie können ebenso wie diese Berichte von den Gruppen "Eigene Berichte" und "Benutzerberichte" kopiert, entfernt, exportiert werden usw. Weitere Informationen finden Sie unter "Berichte" im Kapitel "Verwalten von Inventar und Berichten".

Ausführen von Berichten

Sie können jeden Bericht aus dem Fenster "Berichte" ausführen. Im Fenster "Berichte" klicken Sie mit der rechten Maustaste auf den gewünschten Bericht, anschließend klicken Sie auf **Ausführen** (Sie können auch die Schaltfläche **Ausführen** in der Symbolleiste verwenden). Die Berichtsdaten werden in der Berichtsansicht angezeigt.

Kapitel 14: Verwenden des Zusatzprodukts zur Inventarverwaltung

Inventarverwaltung

Die Seite "Inventar" enthält eine Aufstellung aller Inventargruppen und -typen. Sie können Gruppen erweitern und ausblenden, indem Sie auf den Gruppennamen oder die Verknüpfungen "Alle erweitern" und "Alle ausblenden" klicken.

Der Begriff "Inventar" bezeichnet Elemente oder Dinge in Ihrem Besitz, die sich - mit Ausnahme der Inventartypen "Computer" und "Software" - nicht elektronisch in die Core-Datenbank scannen lassen, deren Verwendung Sie jedoch verfolgen und verwalten möchten (beispielsweise Drucker, Bildschirme, Telefone, Schreibtische, Büromittel etc.). Es gibt, was die Anzahl oder Arten von Inventargegenständen betrifft, die Sie mit der Inventarverwaltung erfassen können, keine Einschränkungen

Inventar*typen* entsprechen den Dateneingabeformularen, mit denen Inventarelemente in die Datenbank eingegeben werden. Sie können die vordefinierten Inventartypen verwenden oder eigene erstellen.

Auf jeder der Seiten eines Typs können Sie Folgendes tun:

- Typen nach Untergruppen sowie nach globalen Listen sortiert anzeigen.
- Untergruppen erstellen, bearbeiten und löschen, indem Sie auf die Verknüpfung Untergruppen verwalten klicken.
- Die Anzahl der Elemente überprüfen, die gegenwärtig für die einzelnen Typen in der Datenbank registriert sind.
- Die ausgewählte Gruppen- oder Typansicht drucken.
- In der Liste nach Typen suchen.
- Die Details des Typs bearbeiten, indem Sie auf das Bleistiftsymbol klicken.
- Typen löschen, indem Sie auf das X-Symbol klicken. (Ein Typ kann nur gelöscht werden, solange keine Elemente für ihn aufgezeichnet wurden.)
- Neue Typen in einer Untergruppe erstellen, indem Sie auf die Verknüpfung "Typ hinzufügen" klicken.
- Durch Klicken auf den Typnamen eine Liste mit allen Elementen anzeigen, die für einen bestimmten Typ zur Datenbank hinzugefügt wurden.
- Elemente zur Datenbank hinzufügen, indem Sie auf das Pluszeichen (+) der Verknüpfung "Hinzufügen" klicken und das Dateneingabeformular ausfüllen.

Zu den vordefinierten Inventargruppen und -typen gehören:

Verschiedene

- Stuhl
- Benutzer

Büroausstattung

- Kopiergerät
- Digitalkamera
- Faxgerät
- Mobiltelefon
- Telefon
- Projektor
- Fernsehgerät

Technologie

- Computer (ein spezieller Inventartyp mit verknüpften Daten, der aktualisiert und mit in der Core-Datenbank vorhandenen Inventardaten synchronisiert werden kann). Weitere Informationen finden Sie unter "Arbeiten mit Computerinventar".
- Monitor
- PDA
- Drucker
- Router
- Scanner
- Computer (ein spezieller Inventartyp mit verknüpften Daten, der aktualisiert und mit Inventardaten synchronisiert werden kann). Weitere Informationen finden Sie unter "Arbeiten mit Softwareinventar".
- Switch

Arbeiten mit Computerinventar

Der Typ "Computer" ist einer von zwei Inventartypen mit verknüpften Details (Datenfelder), die aktualisiert und mit Informationen aus der Core-Datenbank synchronisiert werden können. Entsprechend gekennzeichnete Computertyp-Details werden mit dem Hardwareinventar eines gescannten Geräts verknüpft (ein gescanntes oder verwaltetes Gerät ist ein Gerät, auf dem der Management Suite-Inventarscanner ausgeführt wurde). Der andere Inventartyp mit verknüpften Details, der sich mit Informationen aus der Core-Datenbank aktualisieren lässt, ist der Softwaretyp.

Sie können verknüpfte Details verwenden, um verknüpfte Datenfelder für Computer zu füllen, die bereits gescannt wurden und einen Inventardatensatz besitzen. Für Computer, die noch nicht mit Ihrem Netzwerk verbunden sind oder noch nicht vom Inventarscanner gescannt wurden, können Sie Computerelemente in der Inventarverwaltung hinzufügen (unter Verwendung einer gültigen MAC-Adresse oder einer vom Hersteller zur Verfügung gestellten Seriennummer); die anderen verknüpften Datenfelder können Sie ausfüllen, nachdem die Rechner gescannt wurden.

Verknüpfte Details für Computer

Nur entsprechend ausgewiesene Computerdetails sind verknüpft und können mit dem Hardwareinventar eines gescannten Computers aktualisiert werden. Diese Details erkennen Sie am verknüpften Detailsymbol. Sie können keine eigenen verknüpften Details für den Inventartyp "Computer" erstellen.

Die folgenden Computerdetails sind verknüpft:

- Inventarkennung (Dieses verknüpfte Detail kann als "Master"-Verknüpfung angesehen werden, da es dazu verwendet wird, jedes spezifische Element des Computerbestandes im Hardwareinventar einwandfrei zu identifizieren, sicherzustellen, dass keine Datensätze doppelt vorhanden sind, und die relevanten verknüpften Daten zu synchronisieren. Die Inventarkennung kann nicht manuell bearbeitet werden.)
- Rechnername
- Hersteller
- MAC-Adresse
- Seriennummer
- Modell
- Inventarkennzeichen
- Domänenname

Alle anderen Details für den Computertyp werden nicht verknüpft und müssen manuell eingegeben und aktualisiert werden.

Sie können manuell Informationen in verknüpfte Datenfelder eingeben, BEVOR Sie die betreffenden Details mit Inventarinformationen aktualisieren. Sobald die verknüpften Daten eines Computers aktualisiert sind, können die verknüpften Datenfelder nicht mehr manuell bearbeitet werden. Sie können jedoch verknüpfte Daten aus dem Inventar so oft aktualisieren, wie Sie möchten.

Nicht verknüpfte Datenfelder können jederzeit in der Inventarverwaltung bearbeitet werden. Nicht verknüpfte Daten werden nicht in der Inventarstruktur eines gescannten Geräts angezeigt.

Aktualisieren verknüpfter Daten für Computer

Sie können von der Seite mit der Computer-Elementliste aus Ihre gesamten gescannten Computer in einem Arbeitsgang aktualisieren (je nachdem, wieviele verwaltete Geräte sich in Ihrer Core-Datenbank befinden, kann dieser Vorgang einige Zeit in Anspruch nehmen). Oder Sie können verknüpfte Daten für einen einzelnen Computer von dessen eigener Seite aus aktualisieren.

So aktualisieren Sie die Computer-Elementliste

1. Öffnen Sie von der Seite "Inventar" aus die Untergruppe **Technologie** und klicken Sie dann auf **Computer**, um das gesamte Computerinventar anzuzeigen, das gegenwärtig in der Datenbank enthalten ist.
2. Klicken Sie auf **Inventardaten aktualisieren**.

Gescannte Geräte, die kein entsprechendes Computerelement auf dieser Seite besitzen, werden zur Liste hinzugefügt, wobei die verknüpften Datenfelder ausgefüllt werden. Wenn keine Daten vorhanden sind, bleibt das Feld leer und kann nicht mehr manuell bearbeitet werden; Sie können es jedoch später im Rahmen eines Aktualisierungsvorgangs füllen.

Wenn bereits ein entsprechendes Computerelement auf dieser Seite existiert, werden dessen verknüpfte Daten mit dem Inventar des gescannten Geräts aktualisiert. Wenn sich die Informationen im Inventar geändert haben, ersetzen die neuen Informationen den Wert in dem verknüpften Datenfeld. Nur verknüpfte Datenfelder werden aktualisiert.

So aktualisieren Sie verknüpfte Daten für ein Computerelement

1. Bearbeiten Sie den Computer von der Seite mit der Computer-Elementliste aus, indem Sie auf das Bleistiftsymbol klicken.
2. Klicken Sie auf **Inventardaten aktualisieren**.

Die verknüpften Daten des Computers werden mit Informationen aus dem entsprechenden Inventar des gescannten Geräts aktualisiert. Hierbei werden alle manuell in ein verknüpftes Datenfeld eingegebenen oder geänderten Werte unter Verwendung des aktuellen Wertes aus dem Inventar neu geschrieben. Leere, verknüpfte Datenfelder werden ausgefüllt, sofern entsprechende Daten existieren. Wenn keine Daten vorhanden sind, bleibt das Feld leer und kann nicht mehr manuell bearbeitet werden; es kann jedoch im Rahmen eines späteren Aktualisierungsvorgangs mit Daten gefüllt werden.

Von einer spezifischen Seite eines Computers aus können Sie auch auf **Inventardaten öffnen** klicken, um die gesamte Inventarstruktur des gescannten Geräts anzuzeigen.

Hinweis: Wenn die Option "Inventardaten öffnen" auf der betreffenden Seite eines Computers nicht zur Verfügung steht, bedeutet dies, dass das Gerät aus dem Hardwareinventar gelöscht wurde. Wenn ein Gerät aus dem Inventar gelöscht wurde, wird dessen Inventardatensatz nicht aus der Inventarverwaltung entfernt.

Arbeiten mit Softwareinventar

Der Typ "Software" ist einer von zwei Inventartypen mit verknüpften Details (Datenfelder), die aktualisiert und mit Informationen aus der Core-Datenbank synchronisiert werden können. Entsprechend gekennzeichnete Details des Inventartyps "Software" werden mit den Lizenzdateiinformationen lizenzierter Softwareprodukte verknüpft. Der andere Inventartyp mit verknüpften Details, der sich mit Daten aus der Core-Datenbank aktualisieren lässt, ist der Computertyp.

Sie können verknüpfte Details verwenden, um damit die verknüpften Datenfelder von Softwareprodukten für Software zu füllen, für die in Software License Monitoring (SLM) in der Hauptkonsole der Managment Suite oder im Abschnitt "Einhaltung" in der Webkonsole eine Lizenzdatei registriert ist. Weitere Informationen zum SML-Tool finden Sie im *Benutzerhandbuch*.

Verknüpfte Details für Software

Nur entsprechend ausgewiesene Softwaredetails sind verknüpft und können von SLM aktualisiert werden. Diese Details erkennen Sie am verknüpften Detailsymbol. Sie können keine eigenen verknüpften Details für den Inventartyp "Software" erstellen.

Die folgenden Softwaredetails sind verknüpft:

- Produktname
- Version
- Herausgeber
- Produkverknüpfungs-ID (Dieses verknüpfte Detail ist eine Art "Master"-Verknüpfung, da es dazu verwendet wird, jeden Softwareinventar-Posten einwandfrei zu identifizieren, sicherzustellen, dass keine Datensätze doppelt vorhanden sind, und die relevanten verknüpften Daten zu synchronisieren. Die Produktverknüpfungs-ID kann nicht manuell bearbeitet werden.)
- Licenznummer
- Lizenztyp
- Menge
- Seriennummer
- Kaufdatum
- Stückpreis
- Bestellnummer
- Wiederverkäufer
- Eigentümer
- Standort
- Hinweis

Alle anderen Details für den Inventartyp "Software" werden nicht verknüpft und müssen manuell eingegeben und aktualisiert werden.

Sie können Informationen manuell in verknüpfte Datenfelder eingeben, BEVOR Sie die betreffenden Details mit SLM-Informationen aktualisieren. Sobald die verknüpften Daten eines Softwareprodukts aktualisiert sind, können die verknüpften Datenfelder nicht mehr manuell bearbeitet werden. Sie können verknüpfte Daten anhand der Produktinformationen in SLM jedoch so oft aktualisieren, wie Sie möchten.

Nicht verknüpfte Datenfelder können jederzeit in der Inventarverwaltung bearbeitet werden.

Aktualisieren verknüpfter Daten für Software

Sie können alle Softwareprodukte, für die Sie eine gültige Lizenzdatei besitzen, in einem Arbeitsgang von der Softwarelementliste aus aktualisieren. Beachten Sie, dass nicht für alle lizenzierten Softwareprodukte in SLM notwendigerweise eine Lizenzdatei existiert. Nur diejenigen lizenzierten Produkte, für die tatsächlich eine Lizenzdatei vorhanden ist, werden aktualisiert. Alternativ hierzu können Sie verknüpfte Daten für ein einzelnes Softwareprodukt (das über eine Lizenzdatei verfügt) von dessen eigener Seite aus aktualisieren.

So aktualisieren Sie die Software-Elementliste

1. Öffnen Sie von der Seite "Inventar" aus die Untergruppe **Technologie** und klicken Sie dann auf **Software**, um das gesamte Softwareinventar anzuzeigen, das gegenwärtig in der Datenbank verzeichnet ist.
2. Klicken Sie auf **Inventardaten aktualisieren**.

Softwareprodukte (mit Lizenzdatei), die kein entsprechendes Softwareelement auf dieser Seite besitzen, werden zur Liste hinzugefügt, wobei die verknüpften Datenfelder gefüllt werden. Wenn keine Daten vorhanden sind, bleibt das Feld leer und kann nicht mehr bearbeitet werden.

Wenn bereits ein entsprechendes Softwareelement auf dieser Seite existiert, werden dessen verknüpfte Daten mit den Lizenzdateidaten in SLM aktualisiert. Wenn sich die Informationen in SLM geändert haben, ersetzen die neuen Informationen den Wert in dem verknüpften Datenfeld. Nur verknüpfte Datenfelder werden aktualisiert. Wenn keine Daten vorhanden sind, bleibt das Feld leer und kann nicht bearbeitet werden.

So aktualisieren Sie verknüpfte Daten für ein Softwareelement

1. Bearbeiten Sie das Softwareprodukt von der Seite aus, in der sich die Liste mit den Softwareelementen befindet, indem Sie auf das Bleistiftsymbol klicken.
2. Klicken Sie auf **Inventardaten aktualisieren**.

Die verknüpften Daten des Softwareprodukts werden mit Daten aus den Lizenzdatei-Informationen des entsprechendes Produkts in SLM aktualisiert. Hierbei werden alle manuell in ein verknüpftes Datenfeld eingegebenen oder geänderten Werte unter Verwendung des aktuellen Wertes in SLM neu geschrieben. Leere, verknüpfte Datenfelder werden ausgefüllt, sofern entsprechende Daten existieren. Wenn keine Daten vorhanden sind, bleibt das Feld leer und kann nicht mehr manuell bearbeitet werden; es kann jedoch im Rahmen eines späteren Aktualisierungsvorgangs mit Daten gefüllt werden.

Verwalten von Verträgen

Die Seite "Verträge" enthält eine Aufstellung aller Vertragsgruppen und -typen. Sie können Gruppen erweitern und ausblenden, indem Sie auf den Gruppennamen oder die Verknüpfungen "Alle erweitern" und "Alle ausblenden" klicken.

Als Vertrag kann jedes beliebige Dokument gelten, das sich auf die formalen Geschäftsbeziehungen Ihres Unternehmens mit Dienstanbietern, Partnern und Herstellern bezieht, deren Daten Sie erfassen und verwalten möchten. Zeichnen Sie wichtige, den Vertrag betreffende Informationen (Namen, Datum des Inkrafttretens, Bestimmungen und Bedingungen, Geschäftsbeziehungen etc.) auf und verknüpfen Sie dann den Vertrag mit dem Inventar, für das der Vertrag gilt. Sie könnten beispielsweise Daten zu einem Leasing-Vertrag für eine Gruppe von Druckern eingeben und dann die Lease mit den Druckern verknüpfen.

Das Hinzufügen von Vertragsinformationen zur Datenbank ist nicht nur hilfreich, weil es die Überwachung Ihres wertvollen Inventars vereinfacht, sondern auch, weil Ihnen auf diese Weise jederzeit wichtige Informationen zur Verfügung stehen, die Sie beim Aushandeln von Bestimmungen und Bedingungen künftiger Verträge benötigen.

Vertrags*typen* repräsentieren die Dateneingabeformulare, die dazu benutzt werden, Vertragselemente in die Datenbank einzugeben. Sie können die vordefinierten Vertragstypen verwenden oder eigene erstellen.

Von jeder Typseite aus können Sie Folgendes tun:

- Typen nach Untergruppen sowie nach globalen Listen sortiert anzeigen.
- Untergruppen erstellen, bearbeiten und löschen, indem Sie auf die Verknüpfung Untergruppen verwalten klicken.
- Die Anzahl der Elemente überprüfen, die gegenwärtig für die einzelnen Typen in der Datenbank registriert sind.
- Die ausgewählte Gruppen- oder Typansicht drucken.
- In der Liste nach Typen suchen.
- Die Details des Typs bearbeiten, indem Sie auf das Bleistiftsymbol klicken.
- Typen löschen, indem Sie auf das X-Symbol klicken. (Ein Typ kann nur gelöscht werden, solange keine Elemente für ihn aufgezeichnet wurden.)
- Neue Typen in einer Untergruppe erstellen, indem Sie auf die Verknüpfung "Typ hinzufügen" klicken.
- Durch Klicken auf den Typnamen eine Liste mit allen Elementen anzeigen, die für einen bestimmten Typ zur Datenbank hinzugefügt wurden.
- Elemente zur Datenbank hinzufügen, indem Sie auf das Pluszeichen (+) der Verknüpfung "Hinzufügen" klicken und das Dateneingabeformular ausfüllen.

Zu den vordefinierten Vertragsgruppen und -typen gehören:

Standard

- Beratervertrag
- Escrow
- Lease

Verwalten von Rechnungen

Die Seite "Rechnungen" enthält eine Aufstellung aller Rechnungsgruppen und -typen. Sie können Gruppen erweitern und ausblenden, indem Sie auf den Gruppennamen oder die Verknüpfungen "Alle erweitern" und "Alle ausblenden" klicken.

Rechnungen sind Dokumente, die den Erwerb, die Ak quisition oder Bezahlung von Produkten und Diensten betreffen. Mithilfe der Inventarverwaltung können Sie Informationen, die eine Rechnung betreffen, eingeben und speichern und mit dem entsprechenden Inventar verknüpfen.

Rechnungs*typen* repräsentieren die Dateneingabeformulare, die dazu benutzt werden, Vertragselemente in die Datenbank einzugeben. Sie können die vordefinierten Rechnungstypen verwenden oder eigene erstellen.

Von jeder Typseite aus können Sie Folgendes tun:

- Typen nach Untergruppen sowie nach globalen Listen sortiert anzeigen.
- Untergruppen erstellen, bearbeiten und löschen, indem Sie auf die Verknüpfung Untergruppen verwalten klicken.
- Die Anzahl der Elemente überprüfen, die gegenwärtig für die einzelnen Typen in der Datenbank registriert sind.
- Die ausgewählte Gruppen- oder Typansicht drucken.
- In der Liste nach Typen suchen.
- Die Details des Typs bearbeiten, indem Sie auf das Bleistiftsymbol klicken.
- Typen löschen, indem Sie auf das X-Symbol klicken. (Ein Typ kann nur gelöscht werden, solange keine Elemente für ihn aufgezeichnet wurden.)
- Neue Typen in einer Untergruppe erstellen, indem Sie auf die Verknüpfung "Typ hinzufügen" klicken.
- Durch Klicken auf den Typnamen eine Liste mit allen Elementen anzeigen, die für einen bestimmten Typ zur Datenbank hinzugefügt wurden.
- Elemente zur Datenbank hinzufügen, indem Sie auf das Pluszeichen (+) der Verknüpfung "Hinzufügen" klicken und das Dateneingabeformular ausfüllen.

Zu den vordefinierten Rechnungsgruppen und -typen gehören:

Standard

- Rechnung
- Bestellung

Verwalten von Projekten

Die Seite "Projekte" enthält eine Aufstellung aller Projektgruppen und -typen. Sie können Gruppen erweitern und ausblenden, indem Sie auf den Gruppennamen oder die Verknüpfungen "Alle erweitern" und "Alle ausblenden" klicken.

Zu großen und komplexen Projekten gehört im Allgemeinen die Anschaffung und Nutzung eines umfangreichen Inventars und der damit verbundenen Materialien. In der Inventarverwaltung können Sie spezifische Projektinformationen in die Datenbank eingeben, das Projekt mit jedem anderen registrierten Element verknüpfen und dann benutzerdefinierte Berichte erstellen, die Sie bei der Verfolgung und Verwalten des Projekts unterstützen.

Projekt*typen* repräsentieren die Dateneingabeformulare, die dazu benutzt werden, Projektelemente in die Datenbank einzugeben. Sie können die vordefinierten Projekttypen verwenden oder eigene erstellen.

Von jeder Typseite aus können Sie Folgendes tun:

- Typen nach Untergruppen sowie nach globalen Listen sortiert anzeigen.
- Untergruppen erstellen, bearbeiten und löschen, indem Sie auf die Verknüpfung Untergruppen verwalten klicken.
- Die Anzahl der Elemente überprüfen, die gegenwärtig für die einzelnen Typen in der Datenbank registriert sind.
- Die ausgewählte Gruppen- oder Typansicht drucken.
- In der Liste nach Typen suchen.
- Die Details des Typs bearbeiten, indem Sie auf das Bleistiftsymbol klicken.
- Typen löschen, indem Sie auf das X-Symbol klicken. (Ein Typ kann nur gelöscht werden, solange keine Elemente für ihn aufgezeichnet wurden.)
- Neue Typen in einer Untergruppe erstellen, indem Sie auf die Verknüpfung "Typ hinzufügen" klicken.
- Durch Klicken auf den Typnamen eine Liste mit allen Elementen anzeigen, die für einen bestimmten Typ zur Datenbank hinzugefügt wurden.
- Elemente zur Datenbank hinzufügen, indem Sie auf das Pluszeichen (+) der Verknüpfung "Hinzufügen" klicken und das Dateneingabeformular ausfüllen.

Zu den vordefinierten Projektgruppen und -typen gehören:

Verschiedene

- Ad-hoc

Standard

- Kapitalausgaben
- Sustaining

Verwalten von globalen Listen

Die Seite "Globale Listen" enthält eine Aufstellung mit allen globalen Listengruppen und -typen. Sie können Gruppen erweitern und ausblenden, indem Sie auf den Gruppennamen oder die Verknüpfungen "Alle erweitern" und "Alle ausblenden" klicken.

Der Begriff "Globale Listen" bezieht sich auf Listen, die Standardinformationen wie Standorte, Firmen und Benutzer enthalten, die global zur Beschreibung von Inventarelementen in Ihrem gesamten Unternehmen verwendet werden können. Indem Sie diese globalen Listen an einer zentralen Stelle definieren und dazu verwenden, Standarddaten zu anderen Typen hinzuzufügen, gewährleisten Sie eine einheitliche Verwendung Ihrer Daten in allen Ihren Inventarverwaltungsdatensätzen. Beispiel: Wenn Sie Daten in einer globalen Liste aktualisieren müssen (wie z.B. den Nachnamen einer Person oder eine Firmenadresse), werden die neuen Informationen automatisch auf alle anderen Elemente übertragen, die diese in globalen Listen geführten Standarddaten beinhalten.

Globale Listen*typen* repräsentieren die Dateneingabeformulare, die dazu benutzt werden, in globalen Listen enthaltene Informationen in die Datenbank einzugeben. Sie können die vordefinierten globalen Listentypen verwenden oder eigene globale Listentypen erstellen.

In einem Dateneingabeformular weist ein Erweiterungs-/Ausblendsymbol neben dem Textfeld eines Datenfelds das Feld als einen globalen Listentyp aus, der dazu verwendet werden kann, ein Detail aus einer Liste der verfügbaren Details dieses globalen Listentyps auszuwählen. Im Gegensatz dazu repräsentiert ein Erweiterungs-/Ausblendsymbol, das sich neben dem Namen eines Datenfelds befindet (an der Stelle, an der es kein Textfeld gibt), ein Tabellendetail.

Hinzufügen eines Details zu einem Typ mithilfe globaler Listen

Globale Listen unterscheiden sich von den Inventar-, Vertrags-, Rechnungs- und Projekttypen, da Sie mit einem globalen Listentyp ein Standarddetail (oder Datenfeld) zu jedem der anderen Typen hinzufügen können. Angenommen, Sie fügen ein Detail zu einem neuen Inventartyp hinzu; durch Auswählen von "Globale Liste" wird ein neues Dialogfeld geöffnet, in dem Sie den globalen Listentyp "Standorte" auswählen können (falls Sie einen Standardwert angeben möchten, können Sie auch einen spezifischen Standort in der Dropdown-Liste mit den verfügbaren Standorten auswählen). In diesem Sinne sind globale Listentypen tatsächlich global einsetzbar, da sie für alle anderen Typen verfügbar sind und standardisierte, einheitliche Informationen in den Inventardatensätzen der Datenbank bereitstellen.

Wenn ein Detail in einer globalen Liste geändert wird, wird diese Änderungen - wie oben bereits erwähnt - auf alle in der Datenbank verzeichneten Elemente übertragen, die dieses Detail verwenden.

Verwenden von globalen Listen zum Ordnen und Anzeigen von Typen

Globale Listen erfüllen noch eine andere Sonderaufgabe in der Inventarverwaltung. Sie lassen sich als übergeordnete Gruppe zum Anzeigen von Listen mit Inventar-, Vertrags-, Rechnungs- und Projekttypen verwenden. Sie können von jeder "Typ"-Seite aus auf die Dropdown-Liste **Gruppieren nach** klicken und eine globale Liste (vordefiniert und benutzerdefiniert) auswählen, nach der die auf dieser Seite aufgeführten Typen geordnet werden sollen.

Wenn Sie beispielsweise Computer-Inventartypen nach Standort anzeigen möchten, wählen Sie die globale Liste "Standort". Alle aktuellen Standorte werden als übergeordnete Gruppe angezeigt, die erweitert werden kann, um die Typen (in ihren Untergruppen) mit entsprechenden Standortdaten anzuzeigen. Typen, die keine Standortdaten enthalten, werden unter der übergeordneten Gruppe "Keine Informationen" aufgelistet. Wenn es im globalen Listentyp "Standort" keine Typen gibt, wird die übergeordnete Gruppe "Keine Informationen" angezeigt, in der alle Untergruppen und Typen der Seite enthalten sind.

Wenn Sie im Menü "Gruppieren nach" **Keine** wählen, werden Untergruppen und Typen ohne eine übergeordnete globale Listengruppe aufgelistet. "Keine" ist die Standardeinstellung.

Wie auf den anderen "Typ"-Seiten können Sie auch von der Seite "Globale Listen" aus Folgendes tun:

- Typen in Untergruppen anzeigen. (Gruppierung nach globalen Listentypen wird auf der Seite "Globale Listen" nicht unterstützt).
- Untergruppen erstellen, bearbeiten und löschen, indem Sie auf die Verknüpfung Untergruppen verwalten klicken.
- Die Anzahl der Elemente überprüfen, die gegenwärtig für die einzelnen Typen in der Datenbank registriert sind.
- Die ausgewählte Gruppen- oder Typansicht drucken.
- In der Liste nach Typen suchen.
- Die Details des Typs bearbeiten, indem Sie auf das Bleistiftsymbol klicken.
- Typen löschen, indem Sie auf das X-Symbol klicken. (Ein Typ kann nur gelöscht werden, solange keine Elemente für ihn aufgezeichnet wurden.)
- Neue Typen in einer Untergruppe erstellen, indem Sie auf die Verknüpfung "Typ hinzufügen" klicken.
- Durch Klicken auf den Typnamen eine Liste mit allen Elementen anzeigen, die für einen bestimmten Typ zur Datenbank hinzugefügt wurden.
- Elemente zur Datenbank hinzufügen, indem Sie auf das Pluszeichen (+) der Verknüpfung "Hinzufügen" klicken und das Dateneingabeformular ausfüllen.

Zu den vordefinierten globalen Listengruppen und -typen gehören:

Standard

- Firma
- Cost-Center
- Abteilung
- Standort
- Lieferant

Erstellen neuer Typen

Verwenden Sie die Seite "Neuen Typ hinzufügen", um eigene benutzerdefinierte Typen für Inventarbestände, Verträge, Rechnungen, Projekte und globale Listen zu erstellen.

Es ist u.U. hilfreich, sich noch einmal zu vergegenwärtigen, dass es sich bei den "Typen" ganz einfach um Dateneingabeformulare handelt (bestehend aus spezifischen Details), die ein Element definieren. Um die Datenverfolgung und Berichterstellung zu vereinfachen, wird zwischen fünf Haupttypen unterschieden: Inventar, Verträge, Rechnungen, Projekte und globale Liste. Ein Drucker ist beispielsweise ein Inventartyp, eine Lease ein Vertragstyp und ein Standort ein globaler, d.h. allgemein anwendbarer Typ. Um bei diesem Beispiel zu bleiben: Der Inventartyp "Drucker" könnte aus Details (Datenfelder) für Hersteller, Modell, Beschreibung, Dienstverlauf (Service History), Garantietyp, Kosten usw. bestehen. Ein Typ dient dazu, Elemente zur Datenbank hinzuzufügen.

Die Inventarverwaltung ist mit mehreren vordefinierten Typen ausgestattet, die dazu verwendet werden können, allgemeine Elemente zur Datenbank hinzuzufügen. Sie besitzen zudem die Flexibilität, so viele zusätzliche benutzerdefinierte Typen zu definieren, wie Sie möchten. Auf diese Weise lässt sich das gesamte Inventar und Informationsaufkommen erfassen, das Sie verwalten möchten.

Alle Typen werden mithilfe des nachstehenden Verfahrens erstellt.

So erstellen Sie einen neuen Typ

1. Klicken Sie in der Inventarverwaltung von einer beliebigen Typseite (Inventar, Verträge, Rechnungen, globale Listen) aus auf die Verknüpfung **Typ hinzufügen**. Die Verknüpfung befindet sich neben der Gruppe, zu der Sie den Typ hinzufügen möchten.
2. Geben Sie in das Feld **Name** einen eindeutigen Namen für den Typ ein.
3. Geben Sie in das Feld **Schlüssel** einen eindeutigen Namen für das Schlüsseldetail ein. Jeder Typ muss mindestens ein als "Schlüssel" ausgewiesenes Detail besitzen, damit er in der Datenbank verfolgt werden kann. Beim ersten Erstellen eines neuen Typs müssen Sie den Namen des Schlüsseldetails angeben.

   Hinweis: Wenn der Schlüssel das einzige Detail für den Typ ist, muss er zudem auch eindeutig und ein obligatorischer Wert sein. Sie können das Schlüsseldetail nicht löschen. Sobald das Schlüsseldetail deklariert ist, können Sie es nicht mehr in ein anderes Detail konvertieren.

4. Wählen Sie in der Dropdown-Liste **Typ** den Informationstyp des Schlüsseldetails. Zu den verfügbaren Typen gehören: Ganze Zahl (Integer), Zeichenfolge (alphanumerische Zeichen oder Symbole), Datum (Datum) und Dezimalwert (Zahl, die zwei Dezimalstellen unterstützt).

   Hinweis: "Statische Liste" und "Globale Liste" sind keine gültigen Informationstypen für das Schlüsseldetail.

5. Wenn Sie den Typ "Zeichenfolge" ausgewählt haben, müssen Sie durch Eingeben eines Zahlenwertes in das Feld **Länge** festlegen, welches Zeichenlimit für die Zeichenfolge gelten soll. Der gültige Bereich umfasst 1 bis 255 Zeichen. Dieses Feld ist ein für Zeichenfolgen obligatorisches Feld und steht anderen Informationstypen nicht zur Verfügung.
6. Wenn Sie den Typ "Zeichenfolge" ausgewählt haben, können Sie ein obligatorisches Format oder eine obligatorische Syntax in das Feld **Eingabemaske** einfügen. Dieses Feld gilt nur für Zeichenfolgen und ist optional.

   Die Eingabemaske signalisiert ein obligatorisches Format beim Eingeben von Daten für dieses Detail in das Dateneingabeformular. Wenn das Detail beispielsweise eine Seriennummer ist, die einem bestimmten Format (z.B. "abc-123456") entsprechen muss, würden Sie folgende Eingabemaske spezifizieren: aaa-######, wobei Folgendes gilt: Das klein geschriebene "a" entspricht jedem beliebigen Buchstaben, der Bindestrich muss übernommen werden und das Fadenkreuz (#) entspricht einer Zahl. Verwenden Sie für den eigentlichen Buchstaben "a" das Format /a und für das eigentliche Fadenkreuzzeichen (#) das Format /#. Diese Maske wird im Dateneingabeformular angezeigt, damit der Benutzer weiß, wie die Daten für das Feld einzugeben sind.

7. Wenn Sie einen Wert angeben möchten, der automatisch im Datenfeld des Schlüsseldetails im Dateneingabeformular angezeigt wird, geben Sie den betreffenden Wert in das Feld **Standardwert** ein. Sie können für jeden beliebigen Informationstyp einen Standardwert eingeben. Die Standardwerte eines Formulars können bearbeitet werden. Dieses Feld ist optional. (Verwenden Sie die Kalender-Schaltfläche, wenn Sie ein Standarddatum eingeben möchten.)
8. Klicken Sie auf **Speichern**, um den Typ und dessen Schlüsseldetail zu speichern, und kehren Sie dann zur Seite "Details für..." zurück. Auf dieser Seite können Sie den Typ weiter konfigurieren, indem Sie zusätzliche Details, Detailtabellen oder Detailvorlagen hinzufügen. Des Weiteren können Sie mithilfe der Dropdown-Liste **Gehört zu** die Untergruppe ändern, in der dieser Typ abgelegt wird.
9. **Wichtig:** Wenn Sie mit dem Konfigurieren fertig sind, müssen Sie zusätzlich auf **Details speichern** auf der Seite "Details für..." klicken, um alle Details zu speichern, die Sie zu diesem Typ hinzugefügt haben.

Sobald ein benutzerdefinierter Typ konfiguriert ist, können Sie Folgendes tun:

- Die Details des Typs bearbeiten, indem Sie auf das Bleistiftsymbol klicken.
- Typen löschen, indem Sie auf das X-Symbol klicken. (Ein Typ kann nur gelöscht werden, solange keine Elemente für ihn aufgezeichnet wurden.)
- Elemente zur Datenbank hinzufügen, indem Sie auf das Pluszeichen (+) der Verknüpfung "Hinzufügen" klicken und das Dateneingabeformular ausfüllen.

Verwenden der Detailübersicht

Diese Seite bietet eine Übersicht über alle Details, aus denen sich der oben auf dieser Seite angegebene Typ zusammensetzt. Es sind diese Details, die im Dateneingabeformular für diesen Typ angezeigt werden.

Die Detailübersicht eines jeden Typs ist - abhängig von den Details, die für die Definition des betreffenden Typs verwendet wurden - ein Unikat. Dagegen sind die Tasks, die Sie auf der jeweiligen Detailübersichtsseite ausführen können, nicht typspezifisch.

Von einer Detailübersicht aus können Sie Folgendes tun:

- Alle Details anzeigen, die den ausgewählten Typ definieren.
- Vorhandene Details bearbeiten, indem Sie auf das Bleistiftsymbol neben dem Detailnamen klicken.
- Neue Details für einen Typ erstellen, indem Sie auf die Verknüpfung Details hinzufügen klicken.
- In einem Arbeitsgang eine Gruppe mit Details zu einem Typ hinzufügen, indem Sie auf die Verknüpfung Vorlage wählen klicken.
- Ein Tabellenfeld zu einem Typ hinzufügen, indem Sie auf Tabelle hinzufügen klicken.
- Ein Detail löschen, indem Sie auf das X-Symbol klicken.
- Details in konfigurierbaren Abschnitten organisieren, indem Sie auf Abschnitte verwalten klicken.

Hinweis: Um keine Änderungen zu verlieren, die Sie ggf. an den in dieser Liste geführten Details vorgenommen haben (einschließlich Änderungen an der Detailvorlage und den Detailtabellen), dürfen Sie nicht vergessen, auf **Details speichern** zu klicken. Wenn Sie ein oder mehrere Details hinzufügen, ändern oder löschen und dann auf dieser Seite auf **Abbrechen** klicken, gehen alle Änderungen verloren.

Erläuterungen zu den Detailsymbolen

Die Detailübersichtsseite enthält eine Legende mit Symbolen, die unterschiedliche Merkmale des Details repräsentieren. Detailsymbole werden auf dieser Seite (und auf der Elementseite sowie in den Dateneingabeformularen neben Datenfeldern) in einer Detailübersichtsliste angezeigt.

Die Legende enthält folgende Symbole:

Schlüssel: Gibt an, dass dieses Detail das Schlüsseldetail für diesen Typ ist. Jeder Typ muss ein (!) Schlüsseldetail besitzen, damit er gespeichert werden kann. Schlüsseldetails werden automatisch als eindeutig und erforderlich deklariert. Ein Schlüsseldetail kann weder gelöscht noch geändert werden.

Eindeutig: Gibt an, dass für das Detail beim Ausfüllen des Dateneingabeformulars ein eindeutiger Wert eingegeben werden muss. Wenn Sie einen Eintrag doppelt eingeben, d.h. derselbe Wert in diesem Datenfeld für ein anderes Element existiert, wird eine Fehlermeldung angezeigt. Eindeutige Schlüsseldetails werden automatisch als erforderlich deklariert. Typen können mehrere Details besitzen, die eindeutige Daten erfordern.

Erforderlich: Gibt an, dass für das Detail beim Ausfüllen des Dateneingabeformulars eindeutige Daten eingegeben werden müssen. Ein erforderliches Detail muss nicht notwendigerweise eindeutig sein. Beispiel: Wenn ein Detail als erforderlich, jedoch nicht als eindeutig deklariert wurde, können Sie dieselben Daten für unterschiedliche Elemente in das betreffende Feld in den Dateneingabeformularen eingeben.

Übersicht: Gibt an, dass das Detail als Spaltenüberschrift auf einer Elementlisten-Seite angezeigt wird.

Verknüpft: Gibt an, dass das Detail mit entsprechenden gescannten oder eingegebenen Daten in der Core-Datenbank verknüpft ist. Dieses Merkmal trifft nur auf einige der Details der Inventartypen "Computer" und "Software" zu. Es gilt nicht für die Details der anderen Typen. Für den Inventartyp "Computer" können Sie verknüpfte Daten mit Inventardaten gescannter Geräte und für den Inventartyp "Software" mit Daten, die Sie für lizenzierte Softwareprodukte eingegeben haben, aktualisieren und synchronisieren. Sie können keine eigenen verknüpften Details erstellen.

Hinzufügen von Details

Verwenden Sie diese Seite, um ein neues Detail hinzuzufügen oder ein vorhandenes Detail zu bearbeiten.

Um ein vorhandenes Detail zu bearbeiten, klicken Sie auf das Bleistiftsymbol neben dem Detailnamen. Lesen Sie die Ausführungen im Abschnitt "Regeln zur Bearbeitung von Details" weiter unten, um zu erfahren, welche Informationen Sie in einem gespeicherten Detail bearbeiten können.

Details repräsentieren die Datenfelder in einem Dateneingabeformular für ein Element, das Sie zur Datenbank hinzufügen möchten, um es auf diese Weise mit der Inventarverwaltung überwachen und verwalten zu können.

So fügen Sie ein neues Detail hinzu

1. Klicken Sie von einer beliebigen Detailübersichtsseite aus auf die Verknüpfung **Detail hinzufügen**.
2. Geben Sie in das Feld **Name** einen eindeutigen Namen für das Detail ein.
3. Wählen Sie in der Dropdown-Liste **Typ** den Detailtyp aus. Zu den verfügbaren Typen gehören: Ganzzahl (Integer), Zeichenfolge (alphanumerische Zeichen oder Symbole), Datum (Datum) und Dezimalwert (echte Zahl, die zwei Dezimalstellen unterstützt), Statische Liste (gibt Ihnen die Möglichkeit, eine vordefinierte Liste mit Werten zu erstellen - siehe Schritt 11 unten) und Globale Liste (gibt Ihnen die Möglichkeit, einen der aktuellen globalen Listentypen auszuwählen - siehe Schritt 12 unten).
4. Die Option **Schlüssel** ist nicht verfügbar, da dies nicht das Anfangsdetail ist. Das Schlüsseldetail wird bei der ursprünglichen Erstellung des Typs definiert; Sie können es weder ändern noch entfernen.
5. Wählen Sie die Option **Eindeutig**, wenn Sie im Dateneingabeformular angeben möchten, dass für dieses Detail (Datenfeld im Formular) ein eindeutiger Wert eingegeben werden muss. Mit anderen Worten, unter den in der Datenbank verzeichneten Elementen darf es in diesem Datenfeld keine Doppeleinträge geben.

   Wenn Sie die Option "Eindeutig" wählen, wird automatisch auch die unten beschriebene Option "Erforderlich" ausgewählt. Ein Datenfeld, das die Eingabe eines eindeutigen Wertes verlangt, gilt auch gleichzeitig als erforderliches Feld.

6. Wählen Sie die Option **Erforderlich**, wenn Sie im Dateneingabeformular signalisieren möchten, dass für dieses Detail (Datenfeld im Formular) ein eindeutiger Wert eingegeben werden muss. Sie erkennen ein erforderliches Feld an dem roten "i"-Symbol im Dateneingabeformular. Ein erforderliches Datenfeld muss nicht notwendigerweise mit eindeutigen Daten gefüllt werden.
7. Wenn Sie den Typ "Zeichenfolge" ausgewählt haben, müssen Sie durch Eingeben eines Zahlenwertes in das Feld **Länge** festlegen, welches Zeichenlimit für die Zeichenfolge gelten soll. Der gültige Bereich umfasst 1 bis 4,000 Zeichen. Dieses Feld ist ein erforderliches Feld für Zeichenfolgen und steht anderen Informationstypen nicht zur Verfügung.

8. Wenn Sie den Typ "Zeichenfolge" ausgewählt haben, können Sie ein erforderliches Format/eine erforderliche Syntax in das Feld **Eingabemaske** einfügen. Dieses Feld gilt nur für Zeichenfolgen und ist optional.

   Die Eingabemaske zeigt beim Eingeben von Daten für dieses Detail in das Dateneingabeformular ein erforderliches Format an. Wenn das Detail beispielsweise eine Seriennummer ist, die einem bestimmten Format (z.B. "abc-123456") entsprechen muss, würden Sie folgende Eingabemaske festlegen: aaa-###### - wobei das klein geschriebene "a" einen beliebigen Buchstaben repräsentiert, der Bindestrich ein literales Zeichen ist und das Fadenkreuz (#) einer Zahl entspricht. Verwenden Sie für den eigentlichen Buchstaben "a" das Format /a und für das eigentliche Fadenkreuzzeichen (#) das Format /#. Diese Maske wird im Dateneingabeformular angezeigt, damit der Benutzer weiß, wie die Daten für das Feld einzugeben sind.

9. Wenn Sie einen Wert angeben möchten, der automatisch im Datenfeld dieses Details im Dateneingabeformular angezeigt wird, geben Sie den betreffenden Wert in das Feld **Standardwert** ein. Diese Option gilt für alle Informationstypen und ist keine erforderliche Option. Alle Standardwerte eines Formulars können bearbeitet werden. (Verwenden Sie die Kalenderschaltfläche, wenn Sie ein Standarddatum eingeben möchten.)
10. Wenn dieses Detail auf der Elementlisten-Seite für den von Ihnen zu konfigurierenden Typ angezeigt werden soll, wählen Sie die Option **Übersicht**. Diese Option ist standardmäßig aktiviert. Wenn Sie die Option "Übersicht" deaktivieren, wird dieses Detail nicht auf der Elementlisten-Seite angezeigt.
11. Wenn Sie eine Liste gültiger Dateneinträge für dieses Detail konfigurieren möchten, wählen Sie den Typ **Statische Liste**. Auf der rechten Seite wird ein neues Dialogfeld angezeigt, das es Ihnen gestattet, Werte zur statischen Liste hinzuzufügen. Die Werte, die Sie zu dieser Liste hinzufügen, stehen für dieses Detail in einer Dropdown-Liste im Dateneintragsformular zur Verfügung.

    Um Werte zur statischen Liste hinzuzufügen, geben Sie einfach einen Wert in das Textfeld **Werte hinzufügen** ein und klicken dann auf das Pluszeichen (+). Wenn Sie einen Wert als Standardwert festlegen möchten (wird automatisch im Datenfeld des Details im Dateneingabeformular angezeigt), wählen Sie den Wert aus und klicken dann auf **Als Standardwert festlegen**. Um einen Wert zu entfernen, wählen Sie ihn aus und klicken auf **Entfernen**.

12. Wenn Sie einen globalen Listentyp verwenden möchten, um dieses Detail zu definieren, wählen Sie den Typ **Globale Liste**. Auf der rechten Seite wird ein neues Dialogfeld angezeigt, in dem Sie einen der aktuellen globalen Listentypen auswählen können (siehe "Verwalten von globalen Listen"). Die Werte, die für den ausgewählten Typ zur Datenbank hinzugefügt wurden, stehen für dieses Detail in einer Dropdown-Liste im Dateneingabeformular zur Verfügung.

Globale Listen enthalten allgemeine Informationen, deren Verwendung unternehmensweit standardisiert ist, beispielsweise Anbieter, Benutzer und Standorte. Um dieses Detail mithilfe eines globalen Listentyps zu definieren, wählen Sie zuerst aus der Dropdown-Liste **Gruppe auswählen** die Untergruppe aus, die den gewünschten globalen Listentyp enthält; wählen Sie anschließend in der Dropdown-Liste **Typ auswählen** den globalen Listentyp aus. (Wenn Sie diesem Detail (Datenfeld im Formular) einen Standardwert zuordnen möchten, wählen Sie in der Dropdown-Liste **Als Standard festlegen** einen Wert aus. Beachten Sie, dass diese Liste keine Einträge enthält, solange noch keine Daten für diesen Typ in die Datenbank eingegeben wurden).

13. Wenn Sie mit dem Konfigurieren der Einstellungen und Werte für das Detail fertig sind, klicken Sie auf **Zurück zum Formular**, um das Detail zu speichern und zur Seite "Details für..." zurückzukehren. Oder klicken Sie auf **Abbrechen**, um den Vorgang zu beenden, ohne das Detail zu speichern.
14. Wenn Sie das Detail in einen bestimmten Abschnitt des Formulars einfügen möchten, klicken Sie auf **Abschnitte verwalten** und wählen dann den Abschnitt aus, in dem das Detail angezeigt werden soll. Klicken Sie dann auf **Bearbeiten** und verschieben Sie das Detail in das Feld **Aktuelle Details**. Weitere Informationen finden Sie unter "Ordnen von Details in Abschnitten".
15. **Wichtig:** Vergessen Sie nicht, auch auf der Seite "Detail für..." auf die Schaltfläche **Details speichern** zu klicken, um alle von Ihnen konfigurierten Details zu speichern.

Regeln zur Bearbeitung von Details

Nachdem ein Typ gespeichert wurde, können Sie nur einige der Informationen für die Details, die diesen Typ definieren, bearbeiten.

Denken Sie daran, dass ein Typ mindestens ein Detail, das sogenannte Schlüsseldetail, besitzen muss. Zusätzlich zu diesem Schlüsseldetail kann ein Typ eine beliebige Anzahl von regulären Details (keine Schlüsseldetails) besitzen.

Sowohl für Schlüsseldetails als auch Nicht-Schlüsseldetails gilt, dass Sie, nachdem Sie die Details gespeichert haben, die folgenden Informationsfelder auf der Seite "Detail bearbeiten" nicht mehr bearbeiten können:

- Name
- Typ
- Schlüssel
- Eindeutig
- Erforderlich

Die Möglichkeit zur Bearbeitung der anderen Felder wird bei Schlüsseldetails oder Nicht-Schlüsseldetails unterschiedlich gehandhabt.

Schlüsseldetails

Für ein Schlüsseldetail zeigt die nachstehende Tabelle die Felder auf der Seite "Detail bearbeiten", die je nach ausgewähltem Informationstyp bearbeitet werden können:

Informationstyp	Länge	Eingabemaske	Standardwert	Übersicht
Neue ganze Zahl	Nein	Nein	Ja	Ja
Zeichenfolge	Ja	Ja	Ja	Ja
Datum	Nein	Nein	Ja	Ja
Numerisch	Nein	Nein	Ja	Ja

Nicht-Schlüsseldetails

Für ein Nicht-Schlüsseldetail zeigt die nachstehende Tabelle die Felder auf der Seite "Detail bearbeiten", die je nach ausgewähltem Informationstyp bearbeitet werden können:

Informationstyp	Länge	Eingabemaske	Standardwert	Übersicht	Statische Listenwerte	Globale Liste - Standardwert
Neue ganze Zahl	Nein	Nein	Ja	Ja	Nein	Nein
Zeichenfolge	Ja	Ja	Ja	Ja	Nein	Nein
Datum	Nein	Nein	Ja	Ja	Nein	Nein
Numerisch	Nein	Nein	Ja	Ja	Nein	Nein
Statische Liste	Nein	Nein	Ja	Ja	Ja	Nein
Globale Liste	Nein	Nein	Nein	Ja	Nein	Ja

Hinzufügen von Tabellenfeldern

Verwenden Sie diese Seite um ein Tabellenfeld zu dem von Ihnen ausgewählten Typ hinzuzufügen. Eine Tabelle umfasst ein oder mehrere Details und wird als erweiterbares Datenfeld in einem Dateneintragsformular angezeigt, wobei jedes Detail durch eine separate Spalte in der Tabelle repräsentiert wird.

In einem Dateneintragsformular stellt ein Erweiterungs-/Ausblendsymbol, das sich neben dem Namen eines Datenfelds befindet (an der Stelle, an der es kein Textfeld gibt), ein Tabellendetail dar. Im Gegensatz dazu stellt ein Erweiterungs- /Ausblendsymbol, das sich neben dem Textfeld eines Datenfelds befindet, einen globalen Listentyp dar.

Ein Beispiel für ein Tabellenfeld ist ein Dienstverlauf (Service History) mit Details wie Kosten, Service-Datum, Techniker, Lieferant usw.

Beim Ausfüllen eines Formulars können Benutzer beliebig viele Einträge zu einem Tabellenfeld hinzufügen, indem sie auf das Symbol **Erweitern** sowie auf die Verknüpfung **Hinzufügen** klicken, die Felder ausfüllen und abschließend auf die Verknüpfung **Zur Tabelle hinzufügen** klicken. Dieser Prozess lässt sich so oft wiederholen, wie Sie Einträge zur Tabelle hinzufügen möchten.

Einige vordefinierte Typen (und ihre zugehörigen Dateneintragsformulare) beinhalten vordefinierte Tabellen. Sie können zudem Ihre eigenen benutzerdefinierten Tabellen erstellen und zu Typen hinzufügen. Jede Tabelle ist an den Typ gebunden, zu dem sie hinzugefügt wurde (d.h., sie lässt sich nicht für andere Typen verwenden).

So fügen Sie ein Tabellenfeld zu einem Typ hinzu

1. Klicken Sie von einer beliebigen Detail-Übersichtsseite auf **Tabelle hinzufügen**.
2. Geben Sie in das Feld **Details für** einen eindeutigen Namen für die Tabelle ein.
3. Klicken Sie auf **Detail hinzufügen**, um ein individuelles Detail zu definieren, das als Spalte in der Tabelle angezeigt wird. Eine Tabelle muss mindestens ein Detail (Datenfeld im Formular) enthalten.
4. Sie können auch auf **Vorlage wählen** klicken, um aus einer Liste vorhandener Detailvorlagen eine Vorlage auszuwählen, mit der mehrere Details gleichzeitig zur Tabelle hinzugefügt werden. Jedes Detail wird als separate Spalte in der Tabelle angezeigt.

   Die Details einer Tabelle werden in der Reihenfolge angezeigt, in der sie eingegeben wurden; sie lassen sich nicht verschieben.

5. Wenn Sie mit dem Konfigurieren der Tabelle fertig sind, klicken Sie auf **Details speichern**, um die Tabelle zu speichern. Die neue Tabelle wird in der Detailliste als ein Tabellentyp angezeigt. Die Details werden in der Liste in alphabetischer Reihenfolge geführt, es sei denn, sie gehören zu einem bestimmten Abschnitt.

6. Wenn Sie die Tabellendetails in einen bestimmten Abschnitt des Formulars einfügen möchten, klicken Sie auf **Abschnitte verwalten** und wählen dann den Abschnitt aus, in dem die Tabelle angezeigt werden soll. Klicken Sie dann auf **Bearbeiten** und verschieben Sie die Tabelle in das Feld **Aktuelle Details**. Weitere Informationen finden Sie unter "Ordnen von Details in Abschnitten".
7. **Wichtig:** Klicken Sie erneut auf **Details speichern** (dieses Mal von der Seite mit der Detailübersicht aus), um die vorgenommenen Änderungen zu speichern.

Sobald eine Tabelle konfiguriert ist, können Sie Folgendes tun:

- Die Details einer Tabelle bearbeiten, indem Sie auf das Bleistiftsymbol klicken.
- Eine vorhandene Tabelle löschen, indem Sie auf das X-Symbol klicken.

Verwalten von Detailvorlagen

Verwenden Sie die Seite "Detailvorlagen" zum Anzeigen, Erstellen und Löschen von Detailvorlagen. Detailvorlagen sind Sets oder Gruppen mit Details, die eine einfache und praktische Möglichkeit bieten, mehrere Details auf einmal zu einem Inventartyp hinzuzufügen.

Hinweis: Eine Detailvorlage wird von der Detailübersichtsseite des Typs, nicht von der Seite "Detailvorlage" aus zu einem Typ hinzugefügt. Sie können auch von der Detailübersichtsseite der Tabelle aus eine Detailvorlage zu einer Tabelle hinzufügen.

Die Inventarverwaltung beinhaltet keine vordefinierten Detailvorlagen. Sie können jedoch beliebig viele Detailvorlagen erstellen, um die Erstellung von benutzerdefinierten Typen und Tabellen zu vereinfachen.

So erstellen Sie eine Detailvorlage

1. Klicken Sie vom Inventarverwaltungsmenü in der Webkonsole aus auf **Detailvorlagen**.
2. Klicken Sie auf **Vorlage hinzufügen**.
3. Geben Sie in das Feld **Details für** einen eindeutigen Namen für die Vorlage ein.
4. Fügen Sie beliebig viele Details zur Vorlage hinzu, indem Sie auf **Detail hinzufügen** klicken.
5. Wenn Sie alle gewünschten Details zur Vorlage hinzugefügt haben, klicken Sie auf **Details speichern**, um die Vorlage zu speichern und zur Vorlagenliste zurückzukehren.

Hinweis: Wenn Sie eine Detailvorlage zu einem Inventartyp hinzufügen, werden alle in dieser Vorlage enthaltenen Details als einzelne Details hinzugefügt, nicht gruppiert als Vorlage. Mit anderen Worten, eine Detailübersichtsliste gibt keine Auskunft darüber, ob die Details aus einer Vorlage stammen.

Um eine Detailvorlage zu bearbeiten, klicken Sie auf das Bleistiftsymbol neben dem Namen der Vorlage.

Um eine Detailvorlage zu löschen, klicken Sie auf das X-Symbol neben dem Namen der Vorlage.

Hinzufügen von Detailvorlagen

Sie können Detailvorlagen für einen Typ oder eine Tabelle zu einer Detailübersichtsliste hinzufügen. Detailvorlagen sind Sets oder Gruppen mit Details, die es Ihnen ermöglichen, mehrere Details auf einmal hinzuzufügen.

Detailvorlagen sind an keinen Typ und an keine Tabelle gebunden. Aktuell verfügbare Vorlagen können von jeder Detail-Übersichtsseite aus angezeigt und hinzugefügt werden.

So fügen Sie eine Detailvorlage hinzu

1. Klicken Sie in einer beliebigen Detail-Übersichtsseite (entweder für einen Typ oder eine Tabelle) auf **Vorlage wählen**. Alle vorhandenen Detailvorlagen werden aufgelistet und zeigen alle Details, die in der jeweiligen Vorlage enthalten sind.
2. Suchen Sie die Vorlage, die Sie zur Detailübersicht hinzufügen möchten, und klicken Sie auf **Vorlage hinzufügen**.

   Alle Details, die in der von Ihnen soeben hinzugefügten Vorlage enthalten sind, werden als individuelle Details in der Detailübersicht geführt. Sie werden nicht als aus einer Vorlage stammend gruppiert oder ausgewiesen.

3. Wenn Sie irgendeines der neu hinzugefügten Details in einen bestimmten Abschnitt des Formulars einfügen möchten, klicken Sie auf **Abschnitte verwalten und wählen dann den Abschnitt aus, in dem das Detail angezeigt werden soll. Klicken Sie dann auf Bearbeiten** und verschieben Sie das Detail in das Feld **Aktuelle Details**. Weitere Informationen finden Sie unter "Ordnen von Details in Abschnitten".
4. **Wichtig:** Sie müssen auch auf **Details speichern** auf der Seite "Detail für..." klicken, um alle von Ihnen konfigurierten Details zu speichern.

Verwenden einer Elementliste

Die Seite "Elementliste" bietet eine Übersicht über alle Elemente, die in der Datenbank für den oben auf dieser Seite angegebenen Typ verzeichnet sind. Um die Elementlisten-Seite eines Typs einzublenden, klicken Sie auf den Namen des Typs auf den Inventar-, Vertrags-, Rechnungs- und Projektseiten oder den Seiten für globale Listen.

Welche Informationen in der Tabelle auf einer Elementlisten-Seite angezeigt werden, ist davon abhängig, bei welchen Details die Übersichtsoption aktiviert wurde. Ist das Kontrollkästchen "Übersicht" aktiviert, so wird das Detail auf der Elementlisten-Seite angezeigt. Sie können auf die Spaltenüberschriften klicken, um die Liste nach diesem Detail (Datenfeld) zu sortieren.

Um Elemente zur Datenbank hinzuzufügen, klicken Sie auf die Verknüpfung **Hinzufügen** und füllen dann das Dateneingabeformular aus. Weitere Informationen finden Sie unter "Hinzufügen von Elementen".

Um die aufgezeichneten Daten eines Elements zu bearbeiten, klicken Sie auf das **Bleistiftsymbol** und geben neue Daten ein. Während der Bearbeitung enthält das Dateneingabeformular des Elements mehrere zusätzliche Optionen. Weitere Informationen finden Sie unter "Bearbeiten eines Elements".

Um ein Element aus der Liste (und aus der Datenbank zu löschen), klicken Sie auf sein **Bleistiftsymbol** und dann auf **Löschen**.

Zusätzliche Elementlisten-Tasks

Von einer Elementlisten-Seite aus können Sie zudem folgende Tasks ausführen:

- Elemente verknüpfen mit anderen Elementen und verwandeten Informationen.
- Daten importieren für Elemente des ausgewählten Typs.
- Daten exportieren für Elemente des ausgewählten Typs.

Von der Elementlisten-Seite für die beiden Inventartypen "Computer" und "Software" können Sie außerdem folgende Tasks ausführen:

- Entsprechend gekennzeichnete, verknüpfte Details (Datenfelder) mit gescannten Inventar- und SLM-Informationen aus der Core-Datenbank aktualisieren. Weitere Informationen finden Sie unter "Arbeiten mit Computerinventar" und "Arbeiten mit Softwareinventar".

Hinzufügen von Elementen zur Datenbank

Diese Seite dient als Dateneingabeformular für den oben auf dieser Seite angegebenen Typ. Die Inventarverwaltung beinhaltet mehrere vordefinierte Inventar-, Vertrags-, Rechnungs-, Projekt- und globale Listentypen und bietet Ihnen die Möglichkeit, so viele benutzerdefinierte Typen in jeder dieser Kategorien zu erstellen wie von Ihnen gewünscht.

Beim Eingeben und Speichern der Informationen in das Dateneingabeformular wird das Element in der Datenbank erfasst.

Eine sich geringfügig unterscheidende Version dieser Seite wird angezeigt, wenn Sie ein Element bearbeiten. Weitere Informationen finden Sie unter "Bearbeiten eines Elements".

Der Inhalt und das Layout des Dateneingabeformulars werden von den Details und Abschnitten des jeweiligen Typs bestimmt. Weitere Informationen finden Sie unter "Verwenden der Detailübersicht" und "Ordnen von Details in Abschnitten".

Das Hinzufügen von Inventarbeständen — und anderen wichtigen Informationen (wie z.B. Verträge, Benutzer und Projekte) — zur Datenbank ist *eine* Aufgabe von zentraler Bedeutung für jeden Benutzer, der die Vorteile einer proaktiven Inventarverwaltung in vollem Umfang nutzen möchte. Die Inventarverwaltung bietet die Tools, die Sie zur Konfiguration der Inventartypen und der sie definierenden Detailelemente benötigen, damit die betreffenden Daten überwacht und letzendlich analysiert sowie über benutzerdefinierte Inventarberichte für die gemeinsame Nutzung zur Verfügung gestellt werden. Letzlich sind die Vorteile der Inventarverwaltung für Ihr Unternehmen jedoch von der Qualität der aufgezeichneten Daten abhängig. Wenn in einem gut durchdachten und gründlich ausgearbeiteten Dateneingabeformular die meisten Felder leer bleiben, gibt es nur wenig zu verfolgen, sodass auch das Erstellen von Berichten in diesem Fall nur von geringem Nutzen ist. Die aufgezeichneten Daten sind der Schlüsselfaktor und die Dateneingabe deshalb der wichtigste Schritt bei der Implementierung einer effektiven Inventarverwaltungslösung.

Obwohl die in den Dateneingabeformularen abgefragten Informationen variieren können, bleibt der Prozess des Hinzufügens der Daten wie unten beschrieben immer gleich.

So fügen Sie ein Element zur Datenbank hinzu

1. Klicken Sie von einer beliebigen Elementliste aus auf **Hinzufügen**. (Der Zugriff auf die Liste erfolgt, indem Sie auf der Seite "Inventar", "Verträge", "Rechnungen" oder "Projekte" auf den Namen eines Typs klicken). Sie können auf die entsprechende Seite auch zugreifen, indem Sie auf das Pluszeichen (+) der Verknüpfung "Hinzufügen" neben dem jeweiligen Elementtyp klicken.

   Hinweis: Sie können die Abschnitte eines Formulars erweitern oder ausblenden, indem Sie auf den Abschnittsnamen klicken. Beachten Sie auch die Legende am oberen Rand des Formulars, in der Sie sich über die Bedeutung der Symbole informieren können, die neben bestimmten Datenfeldern zu sehen sind. Erklärungen für die Detailsymbole finden Sie im Abschnitt "Erläuterungen zu den Detailsymbole".

2. Füllen Sie die Datenfelder aus. Beim Hinzufügen oder Bearbeiten eines Details werden nur Daten akzeptiert, die dem Feldtyp entsprechen (d.h. nur Ganzzahlen in Ganzzahlfeldern, Textzeichenfolgen in Zeichenfolgefeldern etc.).
3. Um das Element zu speichern und weitere Elemente hinzuzufügen, klicken Sie auf **Speichern und ein weiteres hinzufügen**.
4. Um das Element zu speichern und zur vorherigen Seite zurückzukehren, klicken Sie auf **Speichern und zur Liste zurückkehren**.

Das neue Element wird in der Elementliste angezeigt.

Bearbeiten eines Elements

Beim Bearbeiten eines Elements werden auf dieser Seite zusätzlich folgende Optionen angezeigt:

- **Elemente verknüpfen:** Öffnet die Seite Elemente verknüpfen. Hiermit können Sie Verknüpfungen zwischen dem ausgewählten Element und anderen, in der Datenbank aufgezeichneten Elementen erstellen.
- **Löschen:** Entfernt das Element aus der Elementliste und aus der Datenbank. Wenn Sie ein Element löschen, werden Verknüpfungen, die zu diesem Element führen oder von ihm ausgehen, ebenfalls entfernt. Diese Daten können nicht abgerufen werden, es sei denn, sie wurden von Ihnen zuvor in eine CSV-Datei exportiert.
- **Seitenansicht:** Öffnet eine druckerfreundliche Version dieser Seite in einem separaten Fenster, die vom Browser aus gedruckt werden kann.
- **Zuletzt bearbeitet von:** Hiermit können Sie (am unteren Rand der Seite) den Benutzer anzeigen, der dieses Element zuletzt bearbeitet hat. Zusätzlich hierzu wird der Core Server dieses Benutzers und die Uhrzeit der Bearbeitung angezeigt.

Verknüpfen von Elementen

Mit dieser Seite können Sie Verknüpfungen zwischen dem auf dieser Seite genannten Element und jedem anderen in der Datenbank aufgezeichneten Element anzeigen, erstellen und löschen.

Über Verknüpfungen können Sie Ihr gesamtes Anlagevermögen mit den Elementen, auf denen sich dieses Vermögen stützt (Verträge, Standorte, Benutzer, Projekte usw.), in Beziehung setzen und verfolgen. Sie könnten beispielsweise die in Ihrem Unternehmen verwendeten Drucker mit den für sie existierenden Leasing-Verträgen, PDAS mit ihren Benutzern oder Telefonapparate mit ihren Benutzern, Standorten und Serviceverträgen usw. verknüpfen. Verknüpfungen bieten eine zusätzliche Ebene der Inventarverwaltung.

Hinweis: Die Verknüpfungen können nur von einer tatsächlichen Elementseite aus erstellt werden, nicht von der Seite mit der Elementliste.

Verknüpfungen bestehen zwischen tatsächlichen Elementen in der Datenbank, nicht zwischen Elementtypen. Verknüpfungen sind bidirektional. Mit anderen Worten, wenn Sie eine Verknüpfung erstellen, die von einem Drucker zu einem Vertrag führt, führt dieselbe Verknüpfung auf dieser spezifischen Seite des Vertrags auch vom Vertrag zum Drucker.

Sie können die folgenden Elementtypen miteinander verknüpfen:

- Inventar
- Verträge
- Rechnungen
- Projekte

So erstellen Sie eine Verknüpfung

1. Klicken Sie von einer Elementseite aus auf **Elemente verknüpfen**. (Dies ist auch die Methode, mit der Sie die Verknüpfungen eines Elements anzeigen können.)

   Hinweis: Die Seite "Verknüpfte Elemente" verweist auf das ausgewählte Elemente anhand des Schlüsseldetails für dieses Element.

2. Verwenden Sie das Tool **Suchen**, um nach Elementen zu suchen, die Sie mit dem ausgewählten Element verknüpfen möchten. Aktivieren Sie von der Suchergebnisliste aus die Elemente, die Sie verknüpfen möchten, und klicken Sie dann auf **Zur Liste hinzufügen**.
3. Klicken Sie auf **Speichern**, um die Verknüpfungen zu speichern und zur Elementseite zurückzukehren.
4. Klicken Sie auf **Abbrechen**, um den Vorgang zu beenden, ohne zu speichern.

Um eine Verknüpfung zu löschen, müssen Sie auf das X-Symbol klicken, das neben der Verknüpfung in der Liste angezeigt wird. Beim Entfernen eines Elements werden auch alle Verknüpfungen dieses Elements aus der Datenbank gelöscht.

Auf ein verknüpftes Elemente bezogene Informationen können in Inventarverwaltungsberichte eingefügt werden.

Importieren von Elementen

Die Inventarverwaltung bietet die Möglichkeit, Elemente für Inventar-, Vertrags-, Rechnungs-, Projekt- und globale Listentypen zu importieren. Beispiel: Wenn Sie Informationen, die für alle Drucker gelten, zentral in einem Arbeitsblatt gespeichert haben, könnten Sie Druckerdaten in die Elemente für den Inventartyp "Drucker" importieren.

Durch das Importieren und Exportieren können Sie auf die Inventarverwaltung bezogene Daten mit anderen Datenverfolgungs-, Datenbank- und Berichterstellungstools verwenden.

Da Sie Elemente eines bestimmten Typs importieren, steht die Verknüpfung "Importieren" nur auf der Elementlisten-Seite des Typs zur Verfügung.

Ein Benutzer muss das Recht zur Inventarkonfiguration oder Inventardateneingabe besitzen, um Elemente importieren und exportieren zu können.

Sowohl die Import- als auch die Exportfunktion unterstützt nur CSV-formatierte (kommabegrenzte) Dateien. Sie importieren in einer CSV-Datei enthaltene Daten in einen vorhandenen Typ. CSV-formatierte Dateien können mit anderen Inventarverwaltungswerkzeugen wie Microsoft SQL Server, Oracle, Microsoft Access und Microsoft Excel verwendet werden.

So importieren Sie Elemente in einen vorhandenen Typ

1. Klicken Sie von der Seite "Inventar", "Verträge", "Rechnungen", Projekte" oder "Globale Listen" aus auf den Namen des Elementtyps, in den Sie Elemente importieren möchten.
2. Klicken Sie auf der Elementlisten-Seite auf **Importieren**.
3. Geben Sie den vollständigen Pfad (einschließlich des Dateinamens) der zu importierenden CSV-Datei in das Feld **Dateipfad** ein.
4. Klicken Sie auf die Verknüpfung **Beispiel...**, um eine Liste mit allen Details zu erhalten, die verwendet wurden, um den ausgewählten Typ zu definieren. Diese Ansicht zeigt den Detailnamen und andere Detailmerkmale in einer Spaltenliste an. Der Inhalt und das Format Ihrer Importdatei muss mit den Details in dieser Liste kompatibel sein.

   Die CSV-Datei muss so formatiert sein, dass sie mit den Details (Datenfelder) übereinstimmt, die zur Definition des Typs verwendet wurden. Jede Zeile in der Datei entspricht einer Elementreihe auf der Elementlisten-Seite und enthält die Daten für das betreffende Element - durch Kommas voneinander getrennt. Und jeder kommabegrenzte Wert entspricht einer Spalte auf der Elementlisten-Seite. Eine Zeile muss einen Wert für jedes Detail im Typ enthalten. Wenn der "Typ" beispielsweise" durch zehn Details definiert wurde, muss jede Zeile in der CSV-Datei zehn Werte besitzen (ein Wert darf leer sein, solange er durch Kommas getrennt ist). Des Weiteren müssen die Daten in jedem Wert mit dem Datentyp übereinstimmen, der für das Datenfeld (z.B. Ganzzahl, Zeichenfolge, Datum etc.) angegeben wurde, da andernfalls der Importvorgang misslingt.

Die erste Zeile der CSV-Datei muss die Namen der Details (die den Spaltenüberschriften auf einer Elementlisten-Seite entsprechen) enthalten; die Namen müssen durch Kommas voneinander getrennt sein.

Kurz gesagt: Das Format der Importdatei ist im Prinzip mit dem Layout einer Elementlisten-Seite identisch — d.h., es handelt sich um eine Tabellenliste, in der jede Spalte ein Detail repräsentiert und jede Zeile ein individuelles Element.

5. Um duplizierte Daten zu ignorieren, klicken Sie auf **Ignorieren**. Oder: Um duplizierte Daten zu aktualisieren, klicken Sie auf **Aktualisieren**.

   Wenn Sie auf "Ignorieren" klicken und eine Reihe in der zu importierenden Datei besitzt einen Duplikatschlüssel einer Reihe, die bereits in der Datenbank existiert, wird der Duplikatschlüssel NICHT importiert.

   Wenn Sie auf "Aktualisieren" klicken und eine Reihe in der zu importierenden Datei einen Duplikatschlüssel einer Reihe besitzt, die bereits in der Datenbank existiert, wird der Duplikatschlüssel importiert und anstelle der vorhandenen Reihe eingefügt.

6. Importieren Sie die CSV-Datei, indem Sie auf **Jetzt importieren** klicken.

Sofern korrekt formatiert, werden die in der importierten CSV-Datei enthaltenen Daten zur Datenbank hinzugefügt und auf der Elementlisten-Seite angezeigt.

Exportieren von Elementen

Die Inventarverwaltung bietet die Möglichkeit, Daten für Inventar-, Vertrags-, Rechnungs-, Projekt- und globale Listentypen zu exportieren.

Durch das Importieren und Exportieren können Sie auf die Inventarverwaltung bezogene Daten mit anderen Datenverfolgungs-, Datenbank- und Berichterstellungstools verwenden.

Beim Exportieren eines Typs werden alle Elemente, die gegenwärtig für diesen bestimmten Typ in der Datenbank gespeichert sind, exportiert. Daten können nur von einer Elementlisten-Seite aus exportiert werden.

Ein Benutzer muss das Recht zur Inventarkonfiguration oder Inventardateneingabe besitzen, um Elemente importieren und exportieren zu können.

Daten werden als CSV-Datei (kommabegrenzter Wert) exportiert. Wie im Abschnitt "Importieren von Elementen" erläutert, ist das Format dieser CSV-Datei im Wesentlichen mit dem Layout einer Elementlisten-Seite identisch. Jede Zeile in der Datei repräsentiert dabei einen bestimmten Elementdatensatz, und jeder kommabegrenzte Wert in einer Zeile repräsentiert ein Detail (Datenfeld) für das betreffende Element. Alle Elemente für den ausgewählten Typ werden in eine Datei (typname.csv) exportiert. Wenn der Typ Tabellenfelder enthält, wird jede Tabelle als separate Datei (typname-tabellenname.csv) exportiert.

So exportieren Sie Elemente

1. Klicken Sie von der Seite "Inventar", "Verträge", "Rechnungen", Projekte" oder "Globale Listen" aus auf den Namen des Elementtyps, den Sie exportieren möchten.
2. Klicken Sie auf der Elementlisten-Seite auf **Exportieren**.
3. Wenn Sie eine vorhandene Exportkonfiguration verwenden möchten, wählen Sie sie in der Dropdown-Liste **Konfigurationen** aus.
4. Oder geben Sie die für den ausgewählten Typ zu exportierenden Details manuell ein, indem Sie die Details, die Sie nicht exportieren möchten, deaktivieren (alle Details sind standardmäßig aktiviert).

   Wenn Sie Ihre ausgewählten Details als neue Konfiguration für diesen Typ speichern möchten, geben Sie einen Namen in das Feld **Konfigurationsname** ein und klicken Sie auf **Speichern**. Die Konfiguration wird zur Dropdown-Liste hinzugefügt.

5. Klicken Sie auf **Jetzt exportieren**. Das Exportfenster wird geöffnet. Es enthält eine Aufstellung der CSV-Dateien, die exportiert werden können. (Es werden nur dann mehrere Dateien angezeigt, wenn ein oder mehrere Tabellendetails ausgewählt wurden).
6. Klicken Sie auf die Datei, die Sie exportieren möchten.
7. Klicken Sie im Dialogfenster "Datei-Download" des Browsers auf **Speichern**, wählen Sie einen Zielpfad auf dem lokalen Rechner aus und klicken Sie erneut auf **Speichern**.

8. Klicken Sie auf **Schließen**, wenn das Dialogfeld "Download abgeschlossen" angezeigt wird.
9. Sie können auf weitere Dateien im Exportfenster oder auf **Fenster schließen** klicken.

Verwenden von Inventarverwaltungsberichten

Die Inventarverwaltung umfasst ein Berichterstellungstool, mit dem Sie die von Ihnen in die Datenbank eingegebenen Inventarverwaltungsdaten erfassen und analysieren können.

Das Berichterstellungstool beinhaltet mehrere vordefinierte Inventarverwaltungsberichte, mit den Sie die Daten, die Sie für Ihr Inventar, Ihre Verträge, Rechnungen und Projekte eingegeben haben, analysieren können. Diese vordefinierten Berichte erläutern anhand von Beispielen, wie Sie eigene benutzerdefinierte Berichte erstellen können.

Klicken Sie auf das Bleistiftsymbol, um die Konfiguration eines Berichts anzuzeigen und zu bearbeiten.

Klicken Sie auf den Berichtnamen, um einen Bericht auszuführen und die Ergebnisse anzuzeigen.

Um einen Bericht zu löschen, klicken Sie auf das X-Symbol.

Für die Verwendung von Inventarberichten benötigte Rechte

Ein Benutzer muss entweder das Recht "Inventarkonfiguration" (entspricht einer Administrator-Rolle für Inventarverwaltungsfunktionen und beinhaltet alle Inventarverwaltungsrechte) oder das Recht "Berichte" besitzen, um die Verknüpfung "Berichte" und die Funktionen in der Inventarverwaltung anzeigen und verwenden zu können. Wenn ein Benutzer nur über das Recht zum Eingeben von Inventardaten verfügt, werden die Verknüpfungen "Berichte" im linken Fensterausschnitt der Webkonsole dieses Benutzers nicht angezeigt. Ein Benutzer, der das Recht "Berichte" besitzt, sieht zwar die Verknüpfungen "Inventar", "Verträge", "Rechnungen", "Projekte" und "Globale Listen", kann diese Seiten jedoch nur durchsuchen. Er kann keine Typen, Details oder eigentlichen Elemente erstellen, bearbeiten oder löschen. Weitere Informationen finden Sie unter Rollenbasierten Administration und Inventarverwaltung.

Die Rechte werden den Benutzern von einem LANDesk Administrator mithilfe des Benutzerwerkzeugs in der Hauptkonsole der Management Suite erteilt.

Das Recht "Berichte" für die Inventarverwaltung ist dasselbe Berichtsrecht, das verwendet wird, um Zugriff auf das Berichtswerkzeug in der Hauptkonsole der Management Suite zu erteilen. Beachten Sie, dass keiner der Inventarverwaltungsberichte im Berichterstellungstool der Hauptkonsole der Management Suite verfügbar ist (auch nicht für Benutzer, die das Recht "Bericht" besitzen). Sie können nur über die Webkonsole auf Inventverwaltungsberichte zugreifen.

Verwenden von vordefinierten Inventarverwaltungsberichten

Die Inventarverwaltung enthält mehrere vordefinierte Berichte, die Informationen zu den in der Datenbank aufgezeichneten Inventarelementen, Verträgen, Rechnungen, Projekten und damit verbundenen Informationen sammeln. Verwenden Sie diese Berichte als Beispiel dafür, was Sie mit dem Berichterstellungstool tun können.

- In den letzten 30 Tagen abgeschlossene Ad-hoc-Projekte
- In den letzten 30 Tagen begonnene Ad-hoc-Projekte
- Alle Computer und verknüpften Elemente
- Alle Consulting-Verträge
- Alle Leases und verknüpften Elemente
- Alle Mobiltelefone
- Alle PDAs
- Alle Bestellungen und verknüpften Elemente
- Computer nach Kostencenter
- Computer nach "Angefordertes Datum"
- In den letzten 30 Tagen installierte Computer
- Leases nach Business-Code
- Leases nach Kostencenter-Standort
- In den letzten 30 Tagen abgelaufene Leases
- In 30 Tagen ablaufende Leases
- Bestellungen nach Kostencenter-Standort
- Bestellungen nach Anbieter
- Kostencenter-Standort
- Software nach "Angefordertes Datum"
- In den letzten 30 Tagen installierte Software

Erstellen und Ausführen von benutzerdefinierten Berichten

Sie können eigene benutzerdefinierte Berichte erstellen, bearbeiten, ausführen und drucken.

Es gibt drei verschiedene benutzerdefinierte Berichttypen:

Datumsbericht: Liefert Informationen zu den Elementen, die für einen bestimmten Typ aufgezeichnet wurden, gruppiert nach einem Datumsdetail. Beispiel: Sie können einen benutzerdefinierten Datumsbericht erstellen, der Informationen zu einem Inventarelement auf der Basis des Kaufdatums oder zu einem Vertrag auf der Basis des Datums der Vertragsunterzeichnung sammelt. Die Ergebnisse eines Datumsberichts werden von einem für das Datumsdetail festgelegten Zeitrahmen (mehrere Tage umfassender Bereich) bestimmt. Die zusätzlichen Details, die im Bericht enthalten sind, können von Ihnen angepasst werden.

Übersichtsbericht: Liefert Informationen zu Elementen, die für einen bestimmten Typ aufgezeichnet wurden, gruppiert nach einem beliebigen Detail des Typs. Übersichtsberichte zeigen immer einen Zähler und mindestens ein Detail des Elements an. Die zusätzlichen Details, die im Bericht enthalten sind, können von Ihnen angepasst werden.

Listenbericht: Generiert in einer einfachen Liste Informationen zu den Elementen, die für einen bestimmten Typ aufgezeichnet wurden. Die zusätzlichen Details, die im Bericht enthalten sind, können von Ihnen angepasst werden.

Verwenden Sie das unten beschriebene Verfahren, um einen benutzerdefinierten Bericht zu erstellen und auszuführen:

So erstellen und speichern Sie einen benutzerdefinierten Bericht

1. Klicken Sie von der Seite "Berichte" aus auf die Verknüpfung **Bericht hinzufügen**, die sich auf den Berichttyp bezieht, den Sie erstellen möchten—Datums-, Übersichts- oder Listenbericht.
2. Geben Sie in das Feld **Berichtname** einen eindeutigen Namen für den Bericht ein.
3. Wählen Sie in der Dropdown-Liste **Bericht ausführen für**, ob der Bericht für ein Inventarelement, einen Vertrag, eine Rechnung oder einen Projekttyp erstellt werden soll.
4. Wählen Sie in der Dropdown-Liste **Typ wählen** den Typ aus, für dessen aufgezeichnete Elemente Sie Informationen sammeln möchten. Diese Liste enthält alle aktuell verfügbaren Typen für die ausgewählte Kategorie.

   Wenn Sie einen **Listenbericht** erstellen, fahren Sie mit Schritt 7 fort.

5. Für einen **Datumsbericht**:

   Wählen Sie zunächst in der Dropdown-Liste **Nach Detail gruppieren** das Datumsdetail aus, das als Basis für diesen Bericht dienen soll und nach dem die Elemente in diesem Bericht gruppiert werden. Oder wählen Sie einen globalen Listentyp (in Klammern) und dann das Datumsdetail aus dem Untermenü aus. (Die Dropdown-Liste enthält die gegenwärtig verfügbaren *Datums*details für den ausgewählten Typ sowie alle globalen Listentypen, dessen Datumsdetails der ausgewählte Typ verwendet.)

   Geben Sie dann im Feld **Zeitraum** an, von wie vielen Tagen (vor oder nach heute) Sie das Datum in den Bericht einschließen möchten. Beispiel: 0 (Null) bedeutet heute, -30 bedeutet 30 Tage vor dem heutigen Tag (einschließlich heute) und 30 oder +30 bedeutet 30 Tage nach dem heutigen Tag (einschließlich heute). Der Datumsbericht wird alle Elemente beinhalten, die für diesen Typ aufgezeichnet wurden und deren angegebener Datumswert mit einem Datum innerhalb dieses Fensters oder Zeitraums identisch ist.

6. Für einen **Übersichtsbericht**:

   Wählen Sie zunächst in der Dropdown-Liste **Nach Detail gruppieren** das Datumsdetail aus, auf das Sie diesen Bericht basieren möchten und nach dem die Elemente in diesem Bericht gruppiert werden. Oder wählen Sie einen globalen Listentyp (in Klammern) und dann das Detail aus dem Untermenü aus. (Die Dropdown-Liste enthält *alle* gegenwärtig verfügbaren Details für den ausgewählten Typ und jeden Listentyp, dessen Details der ausgewählte Typ verwendet.)

   Wenn der Übersichtsbereicht nur das oben ausgewählte Detail und einen Elementzähler enthalten soll, deaktivieren Sie das Kontrollkästchen **Details**. Wenn Sie diese Option deaktivieren, werden die Optionen "Spalten anzeigen" und "Verwandte Details" abgeblendet und können nicht mehr ausgewählt werden. Wenn Sie jedoch zusätzliche Informationen für den Übersichtssbericht konfigurieren möchten, stellen Sie sicher, dass **Details** (die Standardeinstellung) aktiviert ist, damit Sie zusätzliche Informationsoptionen festlegen können.

7. Geben Sie mithilfe der Option **Spalten anzeigen** für jedes Element an, welche Spalten (die auf der Elementseite Details anzeigen) in den Bericht eingefügt werden sollen. Sie können beispielsweise festlegen, dass nur das Schlüsseldetail, die Übersichtsdetails oder alle Details in die die Übersicht eingefügt werden.
8. Geben Sie mithilfe der Option **Verwandte Details** an, welche zusätzlichen Informationen Sie für das jeweilige Element in der Übersicht anzeigen möchten. Zu den Optionen, die zusätzlich ausgewählt werden können, gehören "Keine", "Tabellendetails" oder "Verknüpfte Elemente".
9. Klicken Sie auf **Speichern und ausführen**, um diese Berichtkonfiguration zu speichern und die Ergebnisse des Berichts zu generieren. Es wird ein separates Browser-Fenster (Popup-Fenster) geöffnet, das es Ihnen ermöglicht, den Bericht anzuzeigen und zu drucken.
10. Oder klicken Sie auf **Speichern**, um die Berichtkonfiguration zu speichern und zur Seite "Berichte" zurückzukehren, ohne den Bericht auszuführen.

Mit jeder der beiden Speicheroptionen wird der Bericht zur alphabetisch geordneten Liste auf der Seite "Berichte" hinzugefügt.

Auch bei den benutzerdefinierten Berichten können Sie, wie bei den vordefinierten Berichten, eine Berichtkonfiguration anzeigen und bearbeiten, indem Sie auf das Bleistiftsymbol klicken. Und auf die gleiche Weise wie bei den vordefinierten Berichten können Sie den Bericht ausführen, indem Sie auf den Berichtnamen klicken.

Sie können den Bericht mit den entsprechenden Druckeinstellungen des Browsers vom Popup-Fenster des Berichts aus drucken.

Kapitel 15: Verwenden von LANDesk Inventory Manager

LANDesk Inventory Manager ist eine Version der LANDesk Management Suite 8, die nur die folgenden inventarbezogenen Funktionen enthält:

- Inventarscannen und inventarbezogene Konsolenfunktionen
- Benutzerdefinierte Datenformulare
- Softwarelizenzüberwachung
- Nicht verwaltete Geräteerkennung
- Berichte für die oben genannten Funktionen

Die Inventory Manager-Installation auf einem Core Server beinhaltet alle LANDesk Management Suite 8-Komponenten. Wenn Sie einen Core Server mit einem Konto aktivieren, das für Inventory Manager lizenziert ist, sind jedoch die Nicht-Inventory Manager-Funktionen in den Management Suite- und Webkonsolen weder verwendbar noch sichtbar.

Informationen zur Verwendung von Inventory Manager finden Sie in den folgenden Kapiteln und Abschnitten dieses Handbuchs:

- Kapitel 1: Verwenden der LANDesk Management Suite-Konsole. Dieses Kapitel beschreibt die Management Suite-Konsole und die Netzwerkansicht. Die rollenbasierte Administration, Geräteüberwachung und einige der Abschnitte zur Management Suite-Dienstkonfiguration sind nicht relevant.
- Kapitel 2: Konfigurieren von Clients. Die Ausführungen in diesem Kapitel konzentrieren sich auf die Clientkonfigurations und sind zum größten Teil für Inventory Manager nicht von Belang. Der Abschnitt Nicht verwaltete Geräteerkennung trifft jedoch zu.
- Kapitel 3: Verwenden von Abfragen. Die erste Hälfte dieses Kapitels zur Verwendung von Abfragen gilt für Inventory Manager, die Ausführungen in der zweiten Hälfte, die sich mit Directory Manager befassen, sind nicht relevant.
- Kapitel 4: Verwalten von Inventar und Berichten. Der größte Teil dieses Kapitels gilt für Inventory Manager.
- Kapitel 7: Verwenden der Webkonsole. Die Abschnitte "Erste Schritte", "Verwalten von Inventardaten" (jedoch nicht "Benutzerdefinierte Datenformulare") und "Überwachen von Softwarelizenzen" treffen zum größten Teil auf Inventory Manager zu.
- Kapitel 8: Überwachen der Einhaltung von Softwarelizenzbestimmungen. In diesem Kapitel sind fast alle Ausführungen für Inventory Manager von Belang.
- Anhang A: Weitere Inventarvorgänge und Fehlerbehebung. Die meisten Ausführungen in diesem Anhang enthalten nützliche Informationen für Inventory Manager.

Im Allgemeinen lässt sich leicht erkennen, welche Informationen für Inventory Manager nicht von Belang sind. Es handelt sich dabei meist um Abschnitte, in denen Management Suite-Funktionen wie Softwareverteilung und Fernsteuerung beschrieben werden, die nicht Teil von Inventory Manager sind.

Benutzerdefinierte Formulare und Inventory Manager

Management Suite und Inventory Manager enthalten ein Tool für benutzerdefinierte Datenformulare (**Extras** | **Benutzerdefinierte Datenformulare**), mit dem Sie Formulare erstellen und verwalten können. Mithilfe von benutzerdefinierten Datenformularen können Sie Informationen von Benutzern erfassen und in die Core-Datenbank einfügen.

Was die Handhabung von benutzerdefinierten Formularen betrifft, gibt es zwischen Inventory Manager und Management Suite leichte Unterschiede. Zwar werden die Formulare in beiden Programmen auf dieselbe Weise erstellt, im Inventory Manager erhalten Clients ihre Formularaktualisierungen jedoch, wenn sie einen Inventarscan senden; zudem können alle Clients alle verfügbaren Formulare sehen. Die Management Suite gibt Ihnen die Möglichkeit, Formulare gezielt nur an bestimmte Clients zu senden; da Inventory Manager jedoch nicht über die Management Suite-Funktion "Geplante Tasks" verfügt, lässt sich in Inventory Manager eine geplante Formularverteilung nicht realisieren.

Anhang A: Zusätzliche Inventaroperationen und Fehlerkorrektur

LANDesk Management Suite verwendet einen Inventarscanner, um Hard- und Softwaredaten für Clients im Netzwerk zu sammeln. Grundlagen zum Inventarscanner werden in Kapitel 4 "Verwalten von Inventar und Berichten" beschrieben. Dieses Kapitel enthält zusätzliche Informationen zum Scannen von Inventar sowie einige Tipps zur Fehlerbehebung.

In diesem Kapitel erfahren Sie mehr über:

- Scannen von benutzerdefinierten Daten
- Festlegen von Intervall und Verlauf des Softwarescannens
- Scannerbefehlszeilenparameter
- Scannen von eigenständigen Clients mit einer Diskette
- Hinzufügen von Inventardatensätzen zur Core-Datenbank
- Hinzufügen von BIOS-Textzeichenfolgen zur Core-Datenbank
- Erstellen von MIF-Dateien
- Scannen von NetWare-Servern
- Scannen von Mac OS X-Clients
- Scannen von Mac OS 9.2.2-Clients
- Bearbeiten der Datei LDAPPL3.TEMPLATE
- Fehlerbehebung beim Inventarscanner

Scannen von benutzerdefinierten Daten

Der Windows-Inventarscanner (für Windows 95/98 und Windows NT/2000/XP) scannt automatisch die Clientregistrierung auf benutzerdefinierte Daten. Wenn Sie einen Client konfigurieren, installiert Management Suite den folgenden Schlüssel in der Registrierung:

```
HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDESK\INVENTORY\CUSTOM FIELDS
```

Der Inventarscanner scannt stets die Registrierung nach dem Schlüssel "Custom Fields" und nimmt die Daten auf, die er unter diesem Schlüssel findet. Anschließend gibt er die benutzerdefinierten Daten in die Benutzerdefiniert-Felder der Core-Datenbank ein. Der Informationsgehalt spielt keine Rolle. Wenn Sie diese Daten in der Management Suite-Konsole ansehen, werden sie in den Benutzerdefiniert-Feldern angezeigt.

Der Inventarscanner liest zwei Datentypen:

- REG_SZ
- REG_DWORD

Unterschlüssel für Benutzerdefiniert-Felder
Der Inventarscanner nimmt kein Scannen nach Unterschlüsseln unterhalb der Benutzerdefiniert-Felder vor.

Zeichenfolgelänge der Benutzerdefiniert-Felder
ASCII-Zeichenfolgen dürfen 255 Zeichen nicht überschreiten. Mehrbyte-Zeichensatz (MBCS)-Zeichenfolgen müssen eine Länge zwischen 127 und 255 Zeichen haben.

Konfigurieren des Scanners zum Scannen von Registrierungsschlüsseln

Der Inventarscanner kann nach Registrierungsschlüsseln scannen, die Sie festlegen, und ihre Werte zur Core-Datenbank hinzufügen. Dies kann hilfreich sein für angepasste Software, Bestandsinformationen oder andere Daten, die in der Registrierung gespeichert sind und in die Core-Datenbank eingefügt werden sollen.

Um das Registrierungsschlüssel-Scanning zu verwenden, fügen Sie einen Abschnitt ganz am Beginn der Datei LDAPPL3.TEMPLATE mit diesem Format ein:

```
[Registrierungsinfo]
KEY=HKLM, Software\Intel\LANDesk, Version
```

Ändern Sie die Werte nach KEY=, sodass nach dem gewünschten Registrierungsschlüssel gesucht wird. Beachten Sie im obigen Beispiel, dass jedes Registrierungsschlüsselelement durch Kommata abgetrennt ist.

Wenn der Inventarscanner die Registrierungsschlüsseldaten abruft, können Sie sie in der Registrierungskategorie unter "Custom Data" anzeigen.

Festlegen von Intervall und Verlauf des Softwarescannens

Sie können festlegen, wann die Software eines Clients gescannt wird und wie lange das Verlaufsprotokoll der Inventaränderungen auf dem Core Server gespeichert bleibt. Diese Intervalle gelten für jeden Client.

Hinweis: Die *Hardware* eines Clients wird immer beim Starten und beim Verbinden mit dem Netzwerk gescannt.

So legen Sie Einstellungen für das Softwarescannen fest

1. Klicken Sie in der Netzwerkansicht der Konsole auf **Konfigurieren | Dienste | Inventar | Softwareprüfung**.
2. Legen Sie die Häufigkeit der Softwareprüfung fest.
3. Legen Sie fest, wie viele Tage der Verlauf gespeichert werden soll.

Der Core Server und die Softwareprüfung
Diese Funktion betrifft nur Clients. Der Core Server ist nicht betroffen, da er grundsätzlich täglich gescannt wird.

Planen einer Inventarscan-Task

Wenn der Client die LANDesk-Agenten ausführt, können Sie das Tool "Geplante Tasks" verwenden, um einen Inventarscan mithilfe eines vordefinierten Skripts zu planen. Sie können das Inventarscannerskript mit der Schaltfläche "Skript planen" in der Symbolleiste des Fensters "Geplante Tasks" planen.

Das Inventarscannerskript befindet sich im Verzeichnis \Program Files\LANDesk\ManagementSuite\Scripts. Das Skript ist eine Windows-.INI-Datei, die Sie mit einem beliebigen Texteditor bearbeiten können. Wenn Sie die Optionen oder Parameter in diesem Skript ändern möchten, öffnen Sie es, und befolgen Sie die darin enthaltenen Anweisungen.

Scannerbefehlszeilenparameter

Sie können Befehlszeilenparameter zu den Kontexteigenschaften des Inventarscanners (LDISCN32.EXE) hinzufügen, um ihn zu steuern.

Die folgende Tabelle enthält die Scannerbefehlszeilenparameter:

Option	Beschreibung
/NTT=IP	IP-Adresse des Core Servers oder DNS-Name und UDP-Port. Beispiel: /NTT=123.123.123.123:5007 oder /NTT=CORESERVER:5007. Das OS/2-Scanner-Tool LDISCAN2.EXE und das DOS-Scanner-Tool LDISCAN.EXE

	verwenden diesen Parameter nicht.
/NTI=IPX	IPX-Adresse des Core Servers. Beispiel: /NTI =00100302:0040C9B8ODC9:26f5.
/UDP	Scanner kommuniziert über UDP statt über TCP. Kombinieren Sie diesen Schalter mit /NTT=[IP].
/NTN=NetBIOS Lana-Nummer	NetBIOS Lana-Nummer, die der Scanner verwenden sollte.
/NOUI	Erzwingt die Scannerausführung ohne Benutzeroberfläche.
/pt	Deaktiviert das Verringern des Prioritäts-Threads, wenn der /NOUI-Schalter verwendet wird. Bei /NOUI wird der Scanner standardmäßig mit einer geringeren Priorität ausgeführt, sofern Sie nicht diesen Schalter verwenden.
/i=inifile	Gibt den Pfad (HTTP, UNC oder einen Laufwerksbuchstaben) für die Master-LDAPPL3-Datei an. WLDISCAN.EXE und LDISCN32.EXE kopieren außerdem die Datei LDAPPL3, die sie in diesem Pfad finden, in die lokale LDAPPL3.INI-Datei des Clients. Die Scanner vergleichen das Datum der Master-LDAPPL3-Datei mit der lokalen LDAPPL3.INI-Datei. Wenn die Daten nicht übereinstimmen, wird die Masterdatei lokal kopiert.
/d=Verzeichnis	Startet das Scannen im festgelegten Verzeichnis. Standardmäßig wird das Scannen im Stammverzeichnis jeder lokalen Festplatte gestartet.
/L	Die Scanergebnisse werden an den Core Server gesendet, von dem aus der Client konfiguriert wurde. Wenn Sie /L verwenden, ist der Parameter /NTT überflüssig.
/sync	Erzwingt ein vollständiges Scannen, einschließlich eines vollständigen Softwarescans. Vollständige Scandateien können eine Größe von mehreren MB haben.

/n	Durchsucht keine Unterverzeichnisse.
/v	Gibt Statusmeldungen während des Scannens aus, außer während WLDISCAN.
/Z=Zahl der Wiederholungsversuche	Gibt an, wie oft der Scanner versucht, den Scan neu zu senden.
/A=Timeout	Zeit, die der Scanner bis zum Timeout wartet.
/W=Wartezeit in Sekunden	Festgelegte Wartezeit des Scanners in Sekunden, bevor das Scannen gestartet wird.
/? oder /h	Zeigt die Hilfe zur Befehlszeilensyntax an.
/s=Servername	Legt den Core Server fest, auf dem Inventardaten gespeichert werden.
/f	Erzwingt ein Scannen der Software, unabhängig vom Scanintervall, das an der Konsole festgelegt wurde. Legen Sie /f- fest, um ein Scannen der Software zu deaktivieren, unabhängig vom Scanintervall, das an der Verwaltungskonsole festgelegt wurde.
/t=[path]filename	Kopiert den Inhalt der angegebenen Datei in die Core-Datenbank. Verwenden Sie diese Option, um Inventardaten von eigenständigen Clients oder von separaten Inventardateien einzugeben.
/o=[path]filename	Schreibt Inventardaten in die festgelegte Ausgabedatei.
/m	Erstellt eine LDISCAN.MIF-Datei, die nicht im Unicode-Format vorliegt, im Verzeichnis C:/DMI/DOS/MIFS. Diese Datei enthält die Inventardaten, die während des Scannens gefunden wurden.
/muni	(Nur LDISCN32.EXE) Erstellt eine Unicode-LDISCAN.MIF-Datei im Verzeichnis unter MIFPATH der LDAPPL3.INI-Datei. Diese Datei enthält die Inventardaten, die während des Scannens gefunden wurden.

/smbios	Scannt SMBIOS mithilfe von LDISCN32.EXE.

So werden Windows-Clients beim Starten gescannt

1. Platzieren Sie den Inventarscanner in die Startgruppe des Clients.
2. Klicken Sie auf **Datei | Eigenschaften**, und geben Sie diese Parameter in die Befehlszeile ein:

```
/V /S=Servername /NTT oder /NTN oder /NTI =.
```

Scannen von eigenständigen Clients mit einer Diskette

So scannen Sie eigenständige Clients

1. Kopieren Sie das entsprechende Inventarscanner-Tool und eine Softwarebeschreibungsdatei (in der Regel LDAPPL3.INI) auf eine Diskette. (Möglicherweise müssen Sie auch ELOGAPI.DLL, YGREP32.DLL, LOC16VC0.DLL, INV16.EXE, LOC32VC0.DLL, LTAPI.DLL und LDISCN32.EXE kopieren.)
2. Führen Sie das Scannen mit /O= Parameter aus und legen Sie den Pfad und den Dateinamen der Ausgabedatei fest.
3. Geben Sie in der Befehlszeilenaufforderung einen eindeutigen Namen für den Client ein. Dieser Name wird in der Datei LDISCAN.CFG auf dem lokalen Laufwerk des Clients gespeichert. Dieser Name wird auch im Beschreibungsfeld in der Core-Datenbank angezeigt. Beispiele:

```
ldiscn32.exe /f /v /o=c:\%Computername%.scn
```

Hinzufügen von Inventardatensätzen zur Core-Datenbank

Sie können Inventardaten von einem eigenständigen Client oder separaten Inventardateien hinzufügen, indem Sie das Inventarscanner-Tool von der Befehlszeile des Betriebssystems ausführen.

So fügen Sie Inventardatensätze von einer Datei in die Core-Datenbank hinzu

- Führen Sie das Scan-Tool mit den Parametern /S= , /T= und entweder /NTT oder /NTI aus.

Hinzufügen von BIOS-Textzeichenfolgen zur Core-Datenbank

Die LDAPPL3.INI-Datei enthält den Abschnitt [BIOS Info]. Dieser Abschnitt ermöglicht das Suchen nach Informationen im BIOS eines Computers. Sie können einen oder mehrere Einträge in den Abschnitt [BIOS Info] einfügen. Diese Einträge definieren neue Schlüssel in der Core-Datenbank und liefern Parsing-Anweisungen an den Inventarscanner. Mit den Parsing-Anweisungen wird festgelegt, wo in der LDBIOS.TXT nach einer bestimmten Zeichenfolge gesucht werden soll. Mithilfe dieser Anweisungen fügt der Inventarscanner Zeichenfolgen aus der LDBIOS.TXT-Datei in die Core-Datenbank ein.

Der Inventarscanner verwendet eine Parsing-Methode zum Auffinden von BIOS-Informationen. So können Sie nach Informationen suchen, die sich eine oder mehrere Zeilen über oder unter einer angegebenen Textzeichenfolge befinden. Mit einer solchen Suche können Sie nach beliebigen Buchstaben- und Zahlenkombinationen suchen, die Computerhardware zugewiesen sind.

Textzeichenfolgen in LDBIOS.TXT

Bei einem Inventarscan gibt Management Suite die im BIOS verfügbaren Textzeichenfolgen in die Textdatei LDBIOS.TXT aus. Diese verborgene Datei befindet sich im selben Verzeichnis wie die Datei LDISCAN.CFG, standardmäßig im Stammverzeichnis von Laufwerk C:. In LDBIOS.TXT werden alle Zeichenfolgen gespeichert, die vom Scanner erstellt werden. Wenn Sie diese Informationen in der Datenbank speichern möchten, können Sie sie mithilfe des CFGFILES-Parameters in der Datei LDAPPL3.INI als Konfigurationsdatei speichern.

Beispiel von BIOS-Einträgen in der Datei LDAPPL3.INI

Es folgt ein Beispiel des Abschnitts [BIOS Info] in der LDDAPPL3.INI-Datei:

```
[BIOS Info]
StringLength=4
Key = BIOS - Manufacturer
Parameters = AllValues,FirstInstance
Value = AMI|American Megatrends::AMI::BIOS - AMI
Value = Copyright.*Dell::Dell::BIOS - Dell

[BIOS - AMI]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(.*\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = (C).*\(AMI|American Megatrends\)

[BIOS - Dell]
```

```
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(A.+\)::\1
Value = BIOS Version: \(A.+\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = (C).*Dell|[Cc]opyright.*Dell
```

Erläuterungen zu BIOS-Einträgen

Einträge im Abschnitt [BIOS Info] setzen sich wie folgt zusammen:

- **[Abschnittsname]:** Identifiziert eine neue Komponente in der Core-Datenbank.
- **StringLength=:** Gibt die Mindestlänge der zu suchenden Zeichenfolgen an.
- **Key=:** Identifiziert Klasse und Attributnamen der beim Durchsuchen der LDBIOS.TXT-Datei zurückgegebenen Informationen.
- **Parameters=:** Legt die Suchkriterien fest, die dem Scanner mitteilen, wo und wie nach Werten gesucht werden soll, die einem bestimmten Schlüssel zugeordnet sind.
- **Value=:** Gibt den Wert an, der im BIOS gesucht wird. Ein Wert besteht aus drei Teilen, die jeweils durch einen zweifachen Doppelpunkt getrennt sind (::). Bei diesen Werten ist die Groß-/Kleinschreibung zu beachten. Alle Zeichen im Wert, selbst Leerzeichen, werden bei der Suche berücksichtigt, sofern es sich nicht um einen Operator handelt.

Erstellen von MIF-Dateien

Wenn Sie eine MIF-Datei benötigen, in der die Inventardaten eines Clients gespeichert werden, können Sie sie erstellen, indem Sie den entsprechenden Scanner in der Befehlszeile ausführen.

Um eine Unicode-MIF-Datei zu erstellen, verwenden Sie die Option /MUNI. Um eine MIF-Datei zu erstellen, die nicht im Unicode-Format vorliegt, verwenden Sie die Option /M.

So erstellen Sie MIF-Dateien

- Geben Sie Folgendes an einer DOS-Eingabeaufforderung ein:

  ```
  LDISCN32 /MUNI /V
  ```

Scannen von NetWare-Servern

Management Suite verwendet LDISCAN.NLM, um NetWare-Server nach Hard- und Softwaredaten zu scannen. Die Befehlszeilensyntax für LDISCAN.NLM lautet:

```
LOAD LDISCAN[.NLM] INV_SERV=Servername
NTI=IPX-Adresse FILE=path [TIME=#] [SCANNOW] [MIF]
```

Die folgende Tabelle enthält die Befehlszeilenparameter, die Sie mit dem NetWare-Scanner verwenden können.

Option	Beschreibung
INV_SERV = serenade	Leitet die Ergebnisse des Scannens an den festgelegten Server. Auf dem festgelegten Server muss der Inventardienst ausgeführt werden.
NTI = IPX-Adresse	Gibt die IPX-Adresse des Core Servers an, an den die Inventardaten gesendet werden sollen.
FILE = Pfad	Führt den Pfad zur Datei LDAPPL3.INI auf.
TIME = #	Legt die Uhrzeit in ganzen Stunden für das Scannen der Server-Hardware fest. Für die Uhr gilt das folgende Format; 0 = Mitternacht und 23 = 11 Uhr nachts. Konfigurieren Sie Softwarescans unter "Optionen" | "Softwareprüfung". Standard ist 20.00 Uhr.
SCANNOW	Erzwingt einen Core Server-Scan, wenn NM geladen wird.
MIF	Erstellt die LDISCAN.MIF-Datei für den Core Server. Die .MIF-Datei enthält die Inventardaten, die auf dem Server gesammelt wurden.

So laden Sie LDISCAN.NLM auf einen NetWare-Server

- Geben Sie an der Serverkonsole die richtige Syntax in die Befehlszeile LDISCAN.NLM ein.

  Um einen Server täglich zu scannen und seine Inventardaten in der Core-Datenbank auf "Server1" aufzuzeichnen, geben Sie Folgendes ein:

```
LOAD LDISCAN INV_SERV=SERVER1 TIMEWORK
NUMBER:NODE ADDRESS:SOCKET FILERS:MONEYCHANGER
```

  Um LDISCAN.NLM auf einem Server zu entladen, geben Sie Folgendes ein:

```
UNLOAD LDISCAN
```

Planen von NetWare-Serverscans

LDISCAN.NLM-Scans werden täglich durchgeführt, wie im Parameter TIME=# angegeben. Der TIME-Parameter wird im folgenden Format angegeben: 0 = Mitternacht und 23 = 11 Uhr nachts. Standard ist 20.00 Uhr.

So ändern Sie die Zeit für Serverscans

- Fügen Sie den Parameter TIME = # zur Ladeeingabe LDISCAN.NLM von LD_AUTO.NCF hinzu.

Scannen von Mac OS X-Clients

Der Mac OS X-Inventarscanner wird von der Mac OS X-Startgruppe ausgeführt. Bei der ersten Installation von LANDesk-Agenten für OS X müssen Sie die Agentenvoreinstellungen manuell auf jedem Client konfigurieren. Sie müssen mindestens die Option **Überprüfung an Adresse senden** konfigurieren.

Sie können die Scannervoreinstellungen von Mac OS X ändern, indem Sie die **Systemvoreinstellungen** öffnen und die Seite **LANDesk-Client** auswählen. Die Seite "LANDesk-Client" bietet die folgenden Optionen:

- **LDMS-Serveradresse**: Geben Sie die IP-Adresse oder den auflösbaren Namen des Core Servers ein, sodass der Scanner die Inventarscans zur Core-Datenbank senden kann.
- **Überprüfung in Verzeichnis speichern**: Wählen Sie ein Verzeichnis auf diesem Client, in dem Sie die Scandaten speichern möchten. Diese Option ist wichtig, wenn Sie die Adresse des Core Servers oben nicht eingegeben haben. Die Scandaten gehen nicht verloren, sondern werden auf diesem Client für eine künftige Verwendung gespeichert.
- **Softwareüberprüfung erzwingen**: Erzwingt einen Softwarescan, wenn der Hardwarescan durchgeführt wird.

So fügen Sie eine Komponente in einen Inventarscan ein

1. Blättern Sie in den Hard- und Softwarelisten nach unten, um die Komponenten anzuzeigen, die ein Scanner auf diesem Client finden kann.
2. Klicken Sie auf das Kontrollkästchen neben der Hard- oder Softwarekomponente, die Sie scannen möchten. Beim nächsten Hard- oder Softwarescan werden diese Komponenten im entsprechenden Scan berücksichtigt.

Scannen von Mac OS 9.2.2-Clients

Um die Voreinstellungen für den Mac-Inventarscanner zu ändern, öffnen Sie den Mac-Scanner aus **Anwendungen (Mac OS9):LANDesk**. Der Scanner scannt alle lokalen, nicht entfernbaren Datenträger. Sie können einen Scan manuell starten, indem Sie auf die Schaltfläche **Ausführen** klicken.

Wenn Sie das Kontrollkästchen **Scannen in Datei** wählen, speichert der Mac-Inventarscanner einen Scan in eine Textdatei im Ordner "Systemerweiterungen", wobei Datum und Uhrzeit an den Dateinamen angehängt werden.

Auswählen von Macintosh-Komponenten für das Inventar

Der Macintosh-Inventarscanner stellt Komponentenkategorien für Macintosh-Inventarscans zur Verfügung. Sie können auswählen, in welchen Kategorien Inventardaten aufgezeichnet werden sollen.

Die folgende Tabelle enthält die *Hardware*-Komponentenkategorien, die für Macintosh-Clients gescannt werden können.

Hardwarekomponente	Beschreibung
AB-Geräte	Apple Desktop-Bus-Geräte wie Tastaturen und Mäuse.
CPU	Mikroprozessor, Coprozessoren und andere CPU-bezogene Komponenten.
Bildschirme	Alle Bildschirme, die an den Client angeschlossen sind.
NuBus-Boards	Add-on-Boards für NuBus-Slots von Apple.
SCSI-Geräte	Alle SCSI-Festplatten und verketteten SCSI-Geräte.
Volumes	Alle lokalen Festplatten.

Die folgende Tabelle enthält die *Software*-Komponentenkategorien, die für Macintosh-Clients gescannt werden können.

Softwarekomponente	Beschreibung
Anwendungen	Sucht nach allen Softwareanwendungen auf einer lokalen Festplatte.
Desk-Zubehör	Sucht nach allem Desk-Zubehör im Ordner "Apple-Menü" innerhalb des Systemordners.
Treiber	Sucht nach einem Gerätetreiber, der auf dem Client funktionsfähig ist.
Schriftarten	Sucht nach Schriftarten, die im Systemordner geladen sind.

INITs	Sucht nach INITs, die im Systemordner geladen sind.
Systeminfo	Sucht nach der Version und anderen Daten, die zum Betriebssystem und dem verwendeten Netzwerk gehören.

Bearbeiten der Datei LDAPPL3.TEMPLATE

Speziell auf die Scanner-Inventarparameter bezogene Informationen sind in der Datei LDAPPL3.TEMPLATE enthalten. Diese Vorlagendatei erkennt zusammen mit der Datei LDAPPL3 das Softwareinventar eines Clients.

Sie können den Abschnitt [LANDesk-Inventar] der Vorlagendatei bearbeiten, um die Parameter zu konfigurieren, die festlegen, wie der Scanner das Softwareinventar erkennt. Standardmäßig ist LDAPPL3.TEMPLATE im folgenden Verzeichnis auf dem Core Server gespeichert: \Program Files\LANDesk\ManagementSuite\LDLogon

Verwenden Sie diese Tabelle als Richtlinie beim Bearbeiten des Abschnitts [LANDesk-Inventar] in einem Texteditor.

Option	Beschreibung
Modus	Bestimmt, wie der Scanner die Software auf den Clients scannt. Standard ist "Aufgelistete". Einstellungen: • **Aufgelistete:**Zeichnet die in LDAPPL3 aufgelisteten Dateien auf. • **Nicht aufgelistete:**Zeichnet die Namen und Datumsangaben von allen Dateien auf, deren Erweiterungen in der Zeile "ScanExtensions" aufgeführt, jedoch nicht in LDAPPL3 definiert sind. Mit dieser Methode lässt sich nicht autorisierte Software auf dem Netzwerk finden. • **Alle:**Findet aufgelistete und nicht aufgelistete Dateien.
Duplicate	Zeichnet Mehrfachinstanzen von Dateien auf. Setzen Sie den Wert auf OFF, um nur die erste Instanz aufzuzeichnen, oder auf ON, um alle gefundenen Instanzen aufzuzeichnen. Standard ist ON.
ScanExtensions	Legt die Dateierweiterungen fest (.EXE, .COM, .CFG usw.), nach denen gescannt wird. Trennen Sie die Erweiterungen durch ein Leerzeichen voneinander. Standardmäßig werden nur .EXEs gescannt.
Version	Die Versionsnummer der Datei LDAPPL3 .
Revision	Die Revisionsnummer der Datei LDAPPL3, die für zukünftige Kompatibilität sorgt.
CfgFiles 1-4	Zeichnet Datum, Uhrzeit, Dateigröße und Inhalt der entsprechenden Dateien auf. Sie müssen den Laufwerksbuchstaben (z. B. c:) nicht angeben, wenn Sie alle lokalen Laufwerke durchsuchen möchten. Sie

	können mehr als eine Datei auf jeder der vier Zeilen angeben. Die Länge der Zeilen ist jedoch auf 80 Zeichen beschränkt. Trennen Sie Pfadnamen innerhalb derselben Zeile durch ein Leerzeichen voneinander. Der Scanner vergleicht die Daten und die Größe der aktuellen Datei mit der des vorherigen Scans. Wenn Datum und Größe nicht übereinstimmen, zeichnet der Scan den Inhalt der Datei als neuere Revision auf.
ExcludeDir 1-3	Schließt bestimmte Verzeichnisse aus einem Scan aus. Sie müssen den Laufwerksbuchstaben (z. B. c:) nicht angeben, wenn Sie alle lokalen Laufwerke ausschließen möchten. Aufzählungen müssen bei 1 starten und fortlaufend sein. Sie müssen jede Zeile mit "\" beenden.
MifPath	Legt fest, wo MIF-Dateien auf dem lokalen Laufwerk eines Clients gespeichert werden. Der Standardpfad ist c:\DMI\DOS\MIFS.
UseDefaultVersion	Wenn die Einstellung TRUE gewählt wird, meldet der Scanner nur dann eine Übereinstimmung, wenn eine Datei genau mit einem Dateinamens- und Dateigrößeneintrag in LDAPPL3 übereinstimmt (in der Meldung trägt die Version den Namen EXISTS). Dies kann zu falschen Ergebnissen für Anwendungen führen, die einen allgemeinen Dateinamen mit einer unbekannten Anwendung gemeinsam verwenden. In der ursprünglichen Datei LDAPPL3.TEMPLATE ist dieser Parameter auf FALSE festgelegt; d. h., es wird nur dann ein Eintrag hinzugefügt, wenn es sich um eine genaue Übereinstimmung handelt. Wenn der Parameter fehlt, ist die Standardeinstellung TRUE.
SendExtraFileData	Wenn die Einstellung TRUE lautet, werden zusätzliche Dateidaten an den Core Server gesendet. Standard ist FALSE. Dies bedeutet, dass standardmäßig nur Pfad, Name und Version in die Core-Datenbank eingetragen werden.

So bearbeiten Sie die Datei LDAPPL3.TEMPLATE

1. Öffnen Sie auf dem Core Server in Notepad oder einem anderen Texteditor das Verzeichnis LDLogon und LDAPPL3.TEMPLATE.
2. Blättern Sie nach unten zu dem Parameter, den Sie aktualisieren möchten, und nehmen Sie die Änderungen vor.
3. Speichern Sie die Datei.
4. Klicken Sie auf der Konsole auf **Extras | Softwarelizenzüberwachung**.
5. Klicken Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen**, damit den Clients die letzten Änderungen zur Verfügung stehen, wenn sie das nächste Mal einen Inventarscan durchführen, falls der Scannerbefehlszeilenparameter /i auf Clients verwendet wird.

Fehlerbehebung beim Inventarscanner

In diesem Abschnitt werden allgemeine Probleme des Inventarscanners und mögliche Lösungswege beschrieben.

Der Inventarscanner "hängt"

- Achten Sie darauf, dass die alten /DELL- oder /CPQ-Optionen nicht mit in die Befehlszeile eingegeben werden. Management Suite unterstützt diese Optionen nicht mehr.
- Scannen Sie eine Datei mithilfe des Parameters /O=. Möglicherweise zeigt dies einen Konflikt mit der Netzwerkkarte oder dem Netzwerk.
- Wenn der Inventarscanner immer noch hängt, booten Sie den Client neu ohne Speicher-Manager oder andere TSRs, und führen Sie das Scanner-Tool aus. TSR ist die Abkürzung für "Terminate and Stay Resident". In der Regel handelt es sich hierbei um DOS-Programme, die andere Module, die im Speicher ausgeführt werden, laden, beenden oder verlassen.

Hardware eines Clients wird korrekt gescannt, die Software jedoch nicht

- Prüfen Sie, ob die Core-Datenbank so konfiguriert ist, dass ein Softwarescan sofort ausgeführt wird. Verwenden Sie den Parameter /f, um einen Softwarescan zu erzwingen.
- Scannen Sie eine Datei mithilfe des Parameters /O=. Dadurch sollte die Software am Ende der Datei aufgeführt werden.
- Stellen Sie sicher, dass der Client nicht versucht, im CfgFiles-Parameter von LDAPPL3.TEMPLATE in einer Binärdatei zu scannen.

Die Netzwerkansicht enthält nur Inventardaten für einige Clients

Um Clientinformationen anzuzeigen, müssen die Clients in die Core-Datenbank gescannt sein. Clients, die ohne Informationen angezeigt werden, wurden nicht in die Core-Datenbank gescannt.

So zeigen Sie die Inventardaten eines Clients in der Netzwerkansicht an

1. Konfigurieren Sie den Client.
2. Scannen Sie den Client in die Core-Datenbank.

Weitere Informationen zum Konfigurieren von Clients
finden Sie in Kapitel 2 "Konfigurieren von Clients".

Weitere Informationen zum Scannen von Clients
finden Sie in Kapitel 4 "Verwalten von Inventar und Berichten."

Die Prozessorgeschwindigkeit wird nicht richtig oder mit 0 MHz angezeigt

Es gibt keinen Standardaufruf, den eine Anwendung zum Abfragen der Prozessorgeschwindigkeit verwenden kann. Um die Geschwindigkeit eines Prozessors zu ermitteln, überprüfen die Scanner-Tools von Management Suite, wie viele Operationen der Prozessor in einem bestimmten Zeitblock ausführt. Das bedeutet, das Scanner-Tool muss den Prozessortyp kennen, um zu bestimmen, wie viele Operationen der Prozessor pro Sekunde ausführen sollte. Wenn ein Client optimiert wurde oder seine Leistung unter dem Durchschnitt liegt, kann es passieren, dass das Scanner-Tool die Prozessorgeschwindigkeit falsch angibt. Der Unterschied zwischen der tatsächlichen und der angegebenen Geschwindigkeit ist in der Regel gering. Beispielsweise kann bei einem 166-MHz-Client eine Geschwindigkeit von 168 MHz angegeben werden.

Ein Client kann aus einem ähnlichen Grund auch eine Prozessorgeschwindigkeit von 0 MHz angeben. Das Scanner-Tool von Management Suite überprüft anhand einer Tabelle, wie viele Anweisungen ein Prozessor pro Sekunde ausführen sollte. Wenn ein bestimmter Prozessortyp nicht in der Tabelle des Scanner-Tools enthalten ist, gibt das Scanner-Tool 0 MHz zurück.

Steuern von Änderungen der Konfigurationsdatei

Wenn Sie Probleme mit beschädigten Dateien haben, sodass Benutzer an der Ausführung von Windows gehindert werden, verwenden Sie eine .INI-Datei, um die letzten Konfigurationsdateien (z. B. WIN.INI und SYSTEM.INI) für die Clients im Netzwerk zu speichern.

Konfigurieren Sie LDAPPL3.TEMPLATE so, dass nach den gewünschten .INI-Dateien gesucht wird. Richten Sie anschließend Management Suite so ein, dass so viele Revisionen wie gewünscht gespeichert werden.

So geben Sie die Dateien an, die in der Core-Datenbank gespeichert werden sollen

1. Bearbeiten Sie die Datei **\LDMain\LDLogon\LDAPPL3.TEMPLATE** im Editor.
2. Geben Sie die Namen und Pfade der zu erfassenden Dateien durch Leerzeichen getrennt in den Zeilen ein, die mit **CfgFiles** markiert sind.

   Es können maximal 80 Zeichen pro Zeile eingegeben werden. Sie können den Laufwerksbuchstaben weglassen und einen zusätzlichen umgekehrten Schrägstrich ("\") einfügen, wenn alle physischen Laufwerke durchsucht werden sollen.

3. Speichern Sie die Änderungen, und beenden Sie den Editor.

Weitere Informationen zum Bearbeiten der Vorlagendatei finden Sie unter "Bearbeiten der Datei LDAPPL3.TEMPLATE" weiter oben in diesem Kapitel.

So legen Sie die Anzahl der Dateirevisionen fest, die in der Core-Datenbank gespeichert werden soll

1. Klicken Sie auf **Konfigurieren | Dienste | Inventar**.
2. Geben Sie unter Wählen Sie die Anzahl der Tage an, wie viele Tage die Inventarscans gespeichert bleiben sollen.
3. Klicken Sie auf **OK**.

Anhang B: Zusätzliche Informationen zur Betriebssystem-Verteilung und Profilmigration

In diesem Kapitel erfahren Sie mehr über:

Weitere Betriebssystem-Verteilungsverfahren

- Erstellen einer Imaging-Bootdiskette
- Hinzufügen von Anwendungspaketdistributionen an das Ende eines OSD-Skripts
- Verwenden von CSVIMPORT.EXE zum Importieren von Inventardaten
- Erstellen benutzerdefinierter Computernamen
- Anpassen des Abschnitts [RunOnce] der Datei SYSPREP.INF durch Token-Inventarwerte.
- Verwenden von Abbildern in Umgebungen mit Ein- und Multiprozessorsystemen
- Hinzufügen von Treibern für Netzwerkadapter
- Verwenden des LANDesk-Abbildverarbeitungstools für DOS
- Verwenden des LANDesk-Abbildverarbeitungstools für Windows

Hilfe zum Betriebssystem-Verteilung/Migrationstasks-Assistenten

- Seite "Wählen Sie einen Task"
- Seite "Bildverarbeitungs-Task konfigurieren"
- Seite "Skriptdaten eingeben"
- Seite "Geben Sie Berechtigungsnachweise für die Freigabe des Abbildes und Abbildverarbeitungstools ein"
- Seite "Wählen Sie den Abbildspeicherort und das Abbildverarbeitungstool"
- Seite "Zusätzliche Bereitstellungsbefehle eingeben"
- Seite "Multicast-Optionen konfigurieren"
- Seite "Erweiterte Multicast-Optionen konfigurieren"
- Seite "Sysprep-Dateiinformationen angeben"
- Seite "Multiprozessordaten konfigurieren"
- Seite "Generische Sysprep-Optionen angeben"
- Seite "Sysprep-Netzwerkoptionen angeben"
- Seite "Namenskonvention für Zielcomputer zuweisen"
- Seite "Geben Sie Informationen für den Installationsort des LANDesk Management Suite-Client ein"
- Seite "Sammlung für dieses Profil auswählen"
- Informationen zum Dialogfeld "Sammlungsmanager"
- Informationen zum Dialogfeld "Dateiregel"
- Informationen zum Dialogfeld "Regelsammlung"
- Informationen zum Dialogfeld "Benutzerinitiiertes Paket"
- Seite "Geben Sie Berechtigungsnachweise für die Profilspeicherung ein"
- Seite "Geben Sie die DOS-Befehle für die Ausführung auf dem Client ein"

Weitere Betriebssystem-Verteilungsverfahren

Die nachfolgenden Abschnitte enthalten zusätzliche Informationen zu den Abbildungs- und Migrationsfunktionen von LANDesk, die bei der Implementierung dieser Funktionen hilfreich sind.

Erstellen einer Imaging-Bootdiskette

Die LANDesk Betriebssystem-Verteilung (OSD) umfasst ein Dienstprogramm zum Erstellen von Bootdisketten, mit dem Sie mühelos eine Diskette erstellen können, um Clients in Ihrem Management Suite-Netzwerk in einen verwalteten Zustand hochzufahren. Sie können diese Bootdiskette einsetzen, um OSD-Aufträge auf Clients fortzuführen, die kein Betriebssystem besitzen oder aus irgendeinem Grund einen Auftrag nicht ausführen konnten und nun nicht mehr gestartet werden können. Sobald Sie einen Client mit dieser Bootdiskette hochgefahren haben, können Sie einen Auftrag für diesen Client einplanen.

Hinweis: Ein Benutzer muss zum Erstellen einer OSD-Bootdiskette über Administratorrechte auf dem Core Server verfügen (selbst wenn er über die Management Suite OSD-Berechtigung verfügt).

Bootdisketten werden bei ihrer Erstellung mit dem Core Server verknüpft. Falls Sie mehrere Core Server einsetzen, verwenden Sie eine Bootdiskette, die von dem Core Server erstellt wurde, an den der Client berichten soll.

So erstellen Sie eine Imaging-Bootdiskette

1. Klicken Sie auf **Extras | Skripte verwalten**.
2. Klicken Sie im Fenster "Skripte verwalten" auf die Symbolleistenschaltfläche **Bootdiskette erstellen**, um das Dialogfeld "Imaging-Bootdiskette erstellen" zu öffnen.
3. Legen Sie eine 1,44-MB-Diskette in das Diskettenlaufwerk ein, und stellen Sie sicher, dass das Zieldiskettenlaufwerk korrekt ist.

   Hinweis: Alle auf der Diskette vorhandenen Daten werden gelöscht.

4. Wählen Sie den Netzwerkadapter, der von dieser Bootdiskette unterstützt werden soll. Wegen des beschränkten Speicherplatzes kann jede Diskette nur einen Adapter unterstützen.
5. Klicken Sie auf **Start**. Im Statusfeld wird der Verlauf der Diskettenerstellung angezeigt.
6. Nach der Fertigstellung klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Hinzufügen von Anwendungspaketdistributionen an das Ende eines OSD-Skripts

Sie können eine Enhanced Software Distribution- (ESWD-) Anwendungspaketdistribution einfach in ein Betriebssystem-Verteilungsskript aufnehmen.

So fügen Sie ESWD-Pakete einem Betriebssystem-Verteilungsskript hinzu

1. Öffnen Sie das Paketskript im Verzeichnis LANDesk/ManagementSuite/Scripts, und kopieren Sie die Paketdistributionszeilen, die mit REMEXECx= beginnen.
2. Bearbeiten Sie das Skript, indem Sie mit der rechten Maustaste in das Fenster "Skripte verwalten" klicken und dann auf **Erweiterte Bearbeitung** klicken.
3. Fügen Sie die ESW REMEXEC-Befehle am Ende des Skripts ein, und ändern Sie die Nummerierung der REMEXEC-Befehle, sodass die Nummern fortlaufend sind.
4. Fügen Sie vor den eingefügten ESWD-Zeilen eine Zeile für den Befehl LDSLEEP ein, die wie im nachstehenden Beispiel aussehen sollte. Damit wird dem Betriebssystem Zeit gegeben, vor dem Beginn der Paketinstallation den Startvorgang zu beenden.

   REMEXECxx=LDSLEEP.EXE 120

   Ersetzen Sie xx durch eine eindeutige fortlaufende Nummer.

Verwenden von CSVIMPORT.EXE zum Importieren von Inventardaten

Zum Lieferumfang von Management Suite gehört ein Befehlszeilenprogramm, das den Import von Inventardaten in die Core-Datenbank ermöglicht. Dies kann hilfreich sein, wenn Sie neue Clients installieren und über Daten wie MAC-Adressen verfügen. Sie können diese Daten mit CSVIMPORT.EXE in Management Suite importieren, damit Sie Clients frühzeitig als Ziel von Betriebssystem-Verteilungsaufträgen ansprechen können.

CSVIMPORT.EXE benötigt eine Vorlagendatei, die den Inhalt der einzelnen Felder beschreibt und angibt, in welche Core-Datenbankspalten die betreffenden Daten geschrieben werden sollen. Zudem erfordert CSVIMPORT.EXE eine .CSV-Datei mit den Daten, die der von Ihnen angegebenen Vorlagendatei entsprechen. CSVIMPORT.EXE erstellt Miniscan-Dateien, die Sie in das Verzeichnis LANDesk/ManagementSuite/LDScan kopieren können, damit sie der Core-Datenbank hinzugefügt werden.

Beispielvorlagendatei:

Network - NIC Address = %1%
Network - TCPIP - Adapter 0 - Subnet Mask = 255.255.255.0
BIOS - Serial Number = %2%
BIOS - Asset Tag = %3%
Display Name = %4%

Beachten Sie, dass Sie benutzerdefinierte Daten in die Dateien aufnehmen können. Die Einträge %1, %2 usw. beziehen sich auf die Spaltennummer, also die erste Spalte, die zweite Spalte etc. In diesem Beispiel wird die Subnetzmaske 255.255.255.0 für alle Einträge übernommen. Die Spaltenüberschriften der Vorlagendatei müssen den tatsächlichen Feldnamen der Datenbank entsprechen; zusätzliche Informationen sind nicht zulässig.

.CSV-Beispieldatei:

```
0010A4F77BC3, SERIAL11, ASSETTAG-123-1, MACHINE1
0010A4F77BC4, SERIAL21, ASSETTAG-123-2, MACHINE2
0010A4F77BC5, SERIAL31, ASSETTAG-123-3, MACHINE3
0010A4F77BC6, SERIAL41, ASSETTAG-123-4, MACHINE4
0010A4F77BC7, SERIAL51, ASSETTAG-123-5, MACHINE5
0010A4F77BC8, SERIAL61, ASSETTAG-123-6, MACHINE6
```

Rufen Sie CSVIMPORT mit den folgenden drei Parametern auf: <templateFilename> <csvFileName> <outputDirectoryForScanFiles>. Wenn die Ausgabe sofort in die Core-Datenbank eingetragen werden soll, geben Sie Ihr LANDesk/ManagementSuite/LDScan-Verzeichnis als Ausgabeverzeichnis an.

Erstellen benutzerdefinierter Computernamen

Auf der Seite **Namenskonvention für Zielcomputer zuweisen** des Betriebssystem-Verteilung/Migrationstasks-Assistenten können Sie Computernamen definieren, die auf MAC-Adressen, von Ihnen eingegebenem Text und Zählern (nnn..) basieren. Zudem können Sie Namen auf der Grundlage von Inventardaten für Bestandskennzeichen, Seriennummern und Anmeldenamen erstellen, indem Sie in Ihrem Management Suite-Verzeichnis eine Datei namens COMPUTERNAME.INI anlegen.

COMPUTERNAME.INI-Syntax:

```
[Rename Operations]
tok0=ASSET TAG
tok1=SERIAL NUMBER
tok2=LOGIN NAME
```

Die von der .INI-Datei zurückgegebenen Werte ersetzen die $MAC-Token, die in der Seite "Namenskonvention für Zielcomputer zuweisen" des Assistenten angegeben sind.

Sie können lediglich die drei oben genannten Inventarwerte in der Datei verwenden. Die Betriebssystem-Verteilung überprüft die Optionen in der Reihenfolge der tok<x>-Nummerierung. Die Datei muss nicht alle drei der oben genannten Token enthalten. Die erste tok<x>-Option, für die ein gleichbedeutender Datenbankeintrag gefunden wird, ersetzt den $MAC-Token für den abzubildenden Client. Wenn beispielsweise die Datenbank im oben genannten Fall keine Einträge für Bestandskennzeichen (ASSET TAG) oder Seriennummer (SERIAL NUMBER) enthält, aber ein Anmeldename (LOGIN NAME) verzeichnet ist, dann würde der Anmeldename statt des $MAC-Tokens verwendet. Wird keine Übereinstimmung gefunden, dann wird die MAC-Adresse anstelle des $MAC-Tokens eingesetzt.

Die Anmeldenamensoption liefert den Anmeldenamen, der vom letzten Inventarscan zurückgegeben wurde.

Verwenden des nnn-Tokens für Computernamen

Die Seite **Namenskonvention für Zielcomputer zuweisen** des Betriebssystem-Verteilung/Migrationstasks-Assistenten enthält die Option nnn, die, abhängig von der Anzahl der angegebenen n, für eine 3- bis 15-stellige Zahl steht. Die Betriebssystem-Verteilung verwaltet für jede Computernamensvorlage, die Sie im Assistenten angeben, einen fortlaufenden Zähler der verwendeten Nummern. So werden nachfolgende Aufträge dort fortgesetzt, wo der letzte Auftrag endete.

Jede eindeutige Vorlage besitzt einen eigenen Zähler. Wenn Sie immer dieselbe Vorlage verwenden, umfasst der Zähler verschiedene Aufträge. Falls Sie nach der Bereitstellung einiger Clients die Vorlage ändern und später beschließen, wieder die ursprüngliche Vorlage zu verwenden, dann setzt die Zählung für diese Vorlage bei der Nummer ein, die der zuletzt für diese Vorlage verwendeten Nummer folgt.

Anpassen des Abschnitts [RunOnce] der Datei SYSPREP.INF durch Token-Inventarwerte.

Die Datei SYSPREP.INF enthält den Abschnitt [RunOnce], in dem Programme angegeben werden, die ausgeführt werden sollen, nachdem der Client zum ersten Mal gestartet wurde. Wenn Sie diesem Abschnitt eigene Programme hinzufügen, können Sie Datenbanktoken in die Programmbefehlszeile aufnehmen, falls dies für das auszuführende Programm sinnvoll ist. Die Betriebssystem-Verteilung ersetzt die angegebenen Token durch die entsprechenden Core-Datenbankinformationen.

Beispieltoken:

%Computer - Device Name%
%Computer - Login Name%
%Computer - Manufacturer%
%Computer - Model%
%Computer - Type%
%Computer - BIOS - Asset Tag%
%Computer - BIOS - Service Tag%
%Network - TCPIP - Address%
%System - Manufacturer%
%System - Model%
%System - Serial Number%
%Processor - Processor Count%
%Computer - Workgroup%
%Computer - Domain Name%

Sie können mehrere Token miteinander verketten. Beispielsweise lassen sich zwei Token durch einen Doppelpunkt voneinander trennen: %Computer - Workgroup%:%Computer - Device Name% könnte "MeineArbeitsgruppe:MeinComputer" ergeben.

Hinweis: Sie dürfen nur Token verwenden, die einen einzelnen Wert zurückgeben.

Verwenden von Abbildern in Umgebungen mit Ein- und Multiprozessorsystemen

Einprozessor- und Multiprozessor-Clients erfordern verschiedene Windows 2000- und Windows XP-Abbilder. Abhängig von der Hardwarekonfiguration, können Sie möglicherweise ein für ein Einprozessorsystem erstelltes Abbild auch auf einem Multiprozessor-Client verwenden oder umgekehrt.

Clients, die erweiterte Prozessorfunktionen unterstützen, verfügen in der Regel über einen Controller vom Typ APIC (Advanced Programmable Interrupt Controller). Clients, die erweiterte Prozessorfunktionen unterstützen, können zudem mit einer ACPI- (Advanced Configuration and Power Interface-) Schnittstelle ausgestattet sein.

Hinweis: Die Bedingungen, unter denen ein Abbild sowohl für Einprozessor- als auch Multiprozessor-Clients verwendet werden kann, sind kompliziert. Detaillierte Informationen hierzu finden Sie in der Datei UNATTEND.TXT von Microsoft. Im Allgemeinen müssen Sie Folgendes beachten, wenn Sie Abbilder für Einprozessor- und Multiprozessorsysteme gemeinsam nutzen möchten: **Sowohl Quell- als auch Ziel-Clients müssen entweder eine APIC-HAL mit ACPI-Unterstützung oder eine APIC-HAL ohne ACPI-Unterstützung besitzen. Sie können auf einem APIC-Client ohne ACPI-Unterstützung kein ACPI-APIC-Abbild verwenden und umgekehrt auf einem ACPI-APIC-Client kein APIC-Abbild ohne ACPI-Unterstützung**.

So konfigurieren Sie Daten zu mehreren Prozessoren

1. Wählen Sie auf der Seite "Sysprep-Dateiinformationen angeben" des Betriebssystem-Verteilung/Migrationstasks-Assistenten die Option **Erweiterte Multiprozessoroptionen konfigurieren**, und klicken Sie dann auf **Weiter**.
2. Geben Sie auf der Seite "Multiprozessordaten konfigurieren" an, ob Sie ein Abbild von **Windows 2000** oder **Windows XP** bereitstellen.
3. Geben Sie an, ob das verwendete Abbild auf einem **Einprozessor-** oder einem **Multiprozessor-**Client erstellt wurde.
4. Quell- und Ziel-Clients verfügen über dieselbe HAL. Falls das Abbild auf einem APIC-ACPI-Client erzeugt wurde, wählen Sie **APIC**. Wurde das Abbild auf einem APIC-Client ohne ACPI-Unterstützung erstellt, wählen Sie **MPS**.

Hinzufügen von Treibern für Netzwerkadapter

Während eines Betriebssystem-Verteilungsauftrags wird in den folgenden drei Stufen versucht, Treiber für Netzwerkadapter zu erkennen:

Stufe 1 wird unter Windows ausgeführt:

NICINFO.EXE erkennt PnP-Treiber in Windows 2000, XP und Me. Das Programm erkennt auch Windows 9x-Treiber, falls Internet Explorer Version 4.02 oder höher installiert ist. NICINFO.EXE schreibt die erkannte Anbieter- und Gerätekennung in die Datei DOSNIC.INI des virtuellen Boot-Abbilds.

Stufe 2 wird unter DOS ausgeführt:

AUTODETE.EXE sucht nach der von NICINFO.EXE erzeugten Datei DOSNIC.INI und liest Anbieter- und Gerätekennung. Dann schlägt AUTODETE.EXE in der Datei NIC.TXT nach, um den zu ladenden Treiber ausfindig zu machen. Das Programm kopiert den Treiber aus dem Verzeichnis c:\Net\Drivers des virtuellen Boot-Abbilds in das aktuelle RAM-Laufwerksabbild (Standardeinstellung r:\Net). AUTODETE.EXE trägt dann die entsprechenden Daten in die Microsoft-DOS-Konfigurationsdateien für den Netzwerkstapel (SYSTEM.INI und PROTOCOL.INI) ein.

Falls DOSNIC.INI leer ist, durchsucht AUTODETE.EXE alle PCI-Gerätesteckplätze nach Anbieter- und Gerätekennungen für Netzwerkadapter. Falls die gefundene Kennung einem Eintrag in der Datei NIC.TXT entspricht, lädt AUTODETE.EXE den betreffenden Treiber.

Stufe 3 wird unter DOS fortgeführt:

Falls DOSNIC.INI leer ist und AUTODETE.EXE in der Datei NIC.TXT keinen Eintrag findet, der mit der erkannten Kennung übereinstimmt, dann wird der im Betriebssystem-Verteilung/Migrationstasks-Assistenten angegebene Treiber geladen. Falls dieser Treiber nicht geladen werden kann, bleibt der Client in DOS hängen, und Sie müssen ihn von Hand neu starten. Wenn im Assistenten kein Treiber angegeben wurde, legt AUTODETE.EXE eine Datei namens AUTODETE.LOG im Stammverzeichnis des Laufwerks an, und der Client wird wieder mit dem ursprünglichen Betriebssystem hochgefahren.

NICINFO.EXE und AUTODETE.EXE unterstützen keine 16-Bit-PCMCIA-Netzwerkadapter. Sie können Treiber für diese Netzwerkadapter laden, indem Sie, wie für Stufe 3 beschrieben, im Betriebssystem-Verteilung/Migrationstasks-Assistenten den entsprechenden Treiber auswählen. NICINFO.EXE kann Netzwerkadapter erkennen, die CardBus unterstützen.

NICINFO.EXE erfordert PnP-Unterstützung. Windows NT 4 unterstützt PnP-Geräte nicht.

Hinzufügen von Treibern für Netzwerkadapter

So fügen Sie Netzwerkadaptertreiber hinzu, die nicht im Lieferumfang von Management Suite enthalten sind:

1. Bearbeiten Sie die Datei **ALTDRIVERS.INI** im Management Suite-Verzeichnis.
2. Bearbeiten Sie die Datei **NIC.TXT** im Verzeichnis ..\ManagementSuite\OSD\Utilities.
3. Verwenden Sie **COPYFILE.EXE**, um die .DOS- oder .EXE-Treiberdatei in das virtuelle Boot-Abbild unter ..\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG einzufügen.
4. Fügen Sie die Datei **NIC.TXT** mithilfe von **COPYFILE.EXE** in das virtuelle Boot-Abbild ein.

Bearbeiten der Datei ALTDRIVERS.INI

ALTDRIVERS.INI ist die Treiberbeschreibungsdatei.

Beispieleintrag:

[Intel PRO/1000 Adapters]
DRIVER=E1000.DOS
PROTOCOL=E1000

Zwischen [ ] kann eine beliebige Beschreibung stehen. Diese Beschreibung wird im Betriebssystem-Verteilung/Migrationstasks-Assistenten angezeigt, wenn Sie einen Netzwerkadaptertreiber manuell auswählen.

- DRIVER bezeichnet den .DOS- oder .EXE-Netzwerkadaptertreiber.
- PROTOCOL entspricht häufig dem Treibernamen oder dem Herstellernamen.

Bearbeiten der Datei NIC.TXT

Die Datei NIC.TXT enthält Informationen für die Erkennung von Netzwerkadaptern. Sie müssen die Datei NIC.TXT bearbeiten, wenn Sie benutzerdefinierte Adapterdaten hinzufügen möchten. Es folgt ein Beispieleintrag:

ven=115D "Xircom"
dev=0003 "Xircom CardBus Ethernet 10/100 Adapter"
drv="CBENDIS.EXE"
prot="XIRCOM"

Vier Schlüssel und Werte können angegeben werden:

- **ven** umfasst vier Zeichen (zum Beispiel muss 1 in der Form 0001 angegeben werden); die Beschreibung ist beliebig.
- **dev** umfasst vier Zeichen; die Beschreibung ist beliebig.
- **drv** definiert den Treibernamen; als Standarderweiterung wird .DOS eingesetzt.
- **prot** gibt das Protokoll an, ist häufig mit dem Treibernamen oder dem Hersteller identisch.

Wie Sie der Datei NIC.TXT entnehmen können, sind nicht bei allen Treibern alle Schlüssel definiert.

Einfügen von Treiberänderungen in das virtuelle Boot-Abbild

Sie verwenden COPYFILE.EXE, um Treiberänderungen in das virtuelle Boot-Abbild einzufügen. Syntax:

COPYFILE <Abbilddatei> <Quelldatei> <Zieldatei>

Beispiel:

COPYFILE c:\Programme\LANDesk\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG c:\Drivers\MYNIC.DOS\Net\Drivers\MYNIC.DOS

Hinweis: Für die Variable <Zieldatei> muss der Zielpfad ohne den Laufwerksbuchstaben angegeben werden.

Sie müssen den .DOS- oder .EXE-Netzwerkadaptertreiber in das Verzeichnis c:\Net\Drivers und die aktualisierte Datei NIC.TXT in das Verzeichnis C:\Net kopieren.

Verwenden des LANDesk-Abbildverarbeitungstools für DOS

Hinweis: Wenn Sie die Komponente für die Betriebssystem-Verteilung und die Profilmigration installieren, werden automatisch Dateien für das LANDesk-Abbildverarbeitungstool auf dem Core Server installiert. Wenn Sie das LANDesk-Abbildverarbeitungstool von einem anderen Ort ausführen möchten, müssen Sie die folgenden vier Dateien kopieren: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT und BACKALL.BAT.

Das LANDesk Abbildverarbeitungstool für DOS (IMAGE.EXE) ist ein DOS-basiertes Sicherungs- und Wiederherstellungsprogramm, das eine vollständige Statusaufnahme von einer Partition oder einem Datenträger erstellt und direkt auf die meisten ATAPI CD-R/RW-Laufwerke speichert. Sollte diese Partition oder dieser Datenträger jemals unbrauchbar werden, so können Sie ganz einfach das Abbild der Statusaufnahme wiederherstellen.

Beschränkungen

IMAGE.EXE ist für die Verarbeitung von Datenträgerfunktionen auf das BIOS angewiesen. Wenn das Computer-BIOS aus irgendwelchen Gründen den Zugriff auf die Festplatte limitiert und kein Drive Manager zur Verfügung steht, um diese Beschränkung zu korrigieren, dann ist auch IMAGE.EXE Beschränkungen unterworfen.

Systemvoraussetzungen

- IBM-kompatibler Personal Computer mit einem i80386-kompatiblen Mikroprozessor oder größer
- 16 MB RAM
- XMS

Erste Schritte

IMAGE.EXE wird als Teil der LANDesk Betriebssystem-Verteilung im Verzeichnis \Program Files\LANDesk\ManagementSuite\osd\imaging installiert.

Umgebungsvariablen

IMAGE.EXE unterstützt die Verwendung mehrerer unterschiedlicher Umgebungsvariablen:

- **IMSG** blendet eine Meldung auf dem Bildschirm ein. Um mit IMSG eine Meldung zu erstellen, verwenden Sie den Befehl "set" (d.h., set imsg=<eine aus maximal 80 Zeichen bestehende Meldung hier hinzufügen>).
- **IBXT** ändert die Methode, mit der ein Satz CDs gebrannt wird, sodass IMAGE.EXE während einer Wiederherstellung nicht die letzte CD anfordert. Setzen Sie IBXT auf den Wert 1. (d.h., set ibxt=1). Diese Einstellung wird möglicherweise nicht von allen CD-R/RW-Laufwerken unterstützt.

- **IAR** ermöglicht es IMAGE.EXE, beim Schreiben eines Abbilds in eine Datei automatisch auf Benutzereingaben und Fehlermeldung zu reagieren. Setzen Sie IAR auf Y oder N (d.h., set iar=Y). Mit dieser Einstellung werden alle 'Y'es- oder 'N'o-Eingabeaufforderungen, die das Betätigen der Eingabetaste durch den Benutzer erforderlich machen, automatisch beantwortet. Sie können DOS-Fehlerebenen in einer Stapeldatei verwenden, um festzustellen, ob der Vorgang erfolgreich war oder abgebrochen wurde.
- **IOBS=A** testet die Netzwerkgeschwindigkeit und verwendet die beste Puffergröße zum Heraufladen/Herunterladen eines Abbilds.

Befehlszeilenoptionen

IMAGE.EXE unterstützt die Verwendung von Befehlszeilenoptionen. Trennen Sie die Optionen durch Leerzeichen und geben Sie sie in der unten angegebenen Reihenfolge ein. Mit der Befehlszeilenoption /? können Sie eine Liste zusätzlicher Befehlszeilenoptionen anzeigen, die hier nicht erläutert werden.

So erstellen Sie ein komprimiertes Abbild in einer Datei

Format 1: image /Ch# d:\filename.img (keine Validierung)

Format 2: image /Ch#V d:\filename.img (Validierung)

Format 3: image /Ch#VB d:\filename.img (Byte-für-Byte-Validierung)

Erläuterung: Ersetzen Sie das "h" durch die Nummer 0 bis 7 der Quellfestplatte und das # durch die Partitionseintrags-ID. Für die meisten Benutzer ist die Partitions-ID eine Zahl zwischen 1-4; für Datenträger ist sie eine Zahl, die als 0xPVV formatiert wurde, wobei P die erweiterte Partition und VV die Datenträgernummer im Hexadezimalformat von 01 bis FF ist.

Wenn Ihnen die Partitions- oder Datenträger-ID nicht bekannt ist, führen Sie IMAGE.EXE ohne jegliche Befehlszeilenoptionen aus und wählen Sie "Abbild erstellen". Der Bildschirm, in dem die Partitionen und Datenträger aufgelistet werden, zeigt die ID in Klammern als eine Hexadezimalzahl an. Sie sollten dieser Zahl ein 0x in der Befehlszeile voranstellen.

So erstellen Sie ein nicht komprimiertes Abbild in einer Datei

Format 1: image /Ch# /U d:\filename.img (keine Validierung)

Format 2: image /Ch#V /U d:\filename.img (Validierung)

Format 3: image /Ch#VB /U d:\filename.img (Byte-für-Byte-Validierung)

Erläuterung: Wie oben.

So erstellen Sie ein komprimiertes Abbild in einem CD-Laufwerk

Format 1: image /Ch# /CDx (ATAPI)

Format 2: image /Ch# /CDSx (ASPI)

Erläuterung: Die Informationen bzgl. "h" und "#" sind dieselben wie weiter oben. Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x weg (/CD oder /CDS), um eine Geräteliste zu erhalten.

So erstellen Sie ein nicht komprimiertes Abbild in einem CD-Laufwerk

Format 1: image /Ch# /U /CDx (ATAPI)

Format 2: image /Ch# /U /CDSx (ASPI)

Erläuterung: Wie oben.

So stellen Sie ein Abbild aus einer Datei wieder her

Format 1: image /R d:\filename.img (keine Validierung)

Format 2: image /RV d:\filename.img (Validierung nach Bedarf)

Erläuterung: Stellt das Abbild im selben Festplattenlaufwerk und im selben Speicherort wieder her, von dem aus das Abbild erstellt wurde.

So stellen Sie ein Abbild von einer CD wieder her

Format 1: image /R /CDx (ATAPI)

Format 2: image /R /CDSx (ASPI)

Erläuterung: Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x (/CD oder /CDS) aus, um eine Geräteliste zu erhalten.

So limitieren Sie die Dateigröße beim Erstellen

Format: d:\Dateiname;s

Erläuterung: Ersetzen Sie das "s" nach ";" durch 0 für 2 GB, 1 für 698 MB oder 2 für 648 MB.

Punkte zur Beachtung

- Beim Erstellen eines Abbilds sollten Sie die Partition, von der die Sicherungskopie erstellt werden, nicht als Speicherort für die Abbilddatei verwenden. Falls Sie dies tun, wird die Partition zur selben Zeit aktualisiert wie versucht wird, eine Sicherungskopie von ihr zu erstellen. Dies hat zur Folge, dass sich das Dateisystem beim Wiederherstellen der Partition in einem nicht synchronisierten Zustand befindet.
- Das Abbild sollte nicht auf der Partition wiederhergestellt werden, in der sich die Quelldatei für das Abbild befindet. Wenn Sie dies tun, überschreibt die Wiederherstellung die Dateisystemstrukturen und die eigentliche Abbilddatei.
- Nach der Wiederherstellung wird das System neu gestartet. Dies ist erforderlich, da die vom Betriebssystem verwendeten Partitionen und das Dateisystem sich geändert haben. Wird kein Neustart ausgeführt, so nimmt das Betriebssystem an, dass die Partition und das Dateisystem sich im selben Zustand befinden wie vor der Wiederherstellung. Dies kann Datenschäden verursachen. Sie können eine Befehlszeilenwiederherstellung mit /RN überschreiben. /RN sollte jedoch nur von versierten Benutzern verwendet werden, die wissen, dass die Nichtausführung des Neustarts kein Risiko darstellt.

- Beim Durchführen einer Befehlszeilenwiederherstellung wird die wiederhergestellte Partition auf dieselbe Festplattennummer und in dieselbe physikalische Speicherposition auf dem Laufwerk geschrieben, von der aus ihre Sicherungskopie erstellt wurde. Wenn dies ein Datenträger (Volume) war und es jetzt an dieser Speicherposition keine erweiterte Partition gibt, versucht die Wiederherstellung, die ursprüngliche erweiterte Partition zu erstellen. Wenn die erweiterte Partition nicht erstellt werden kann, wir sie als primäre Partition wiederhergestellt. Wenn die Position, von der aus die Partition gesichert wurde, eine primäre Partition war und dieser Stelle jetzt von einer erweiterten Partition belegt wird, wird sie als Datenträger (Volume) wiederhergestellt. Wenn eine vorhandene Partition oder ein Datenträger (Volume) an derselben Stelle beginnt wie die wiederherzustellende Partition, wird eine Warnmeldung eingeblendet, bevor die betreffende Partition oder das Volume überschrieben wird.
- Um den Wiederherstellungsprozess durch Starten der CD auszuführen, benötigen Sie ein ATAPI CD-Laufwerk. Für SCSI-Laufwerke müssen Sie Ihre eigene CDBOOT.F35-Datei erstellen, um die geeigneten DOS ASPI-Treiber zu laden und IMAGE.EXE nach Bedarf über AUTOEXEC.BAT zu starten.

Verwenden des LANDesk-Abbildverarbeitungstools für Windows

Das LANDesk Abbildverarbeitungstool für Windows (IMAGE".EXE) ist ein Windows 32-basiertes Sicherungs- und Wiederherstellungsprogramm, das eine vollständige Statusaufnahme von einer Partition oder einem Datenträger erstellt und direkt auf die meisten DVD+RW oder CD-R/R-Laufwerke speichert. Sollte diese Partition oder dieser Datenträger jemals unbrauchbar werden, so können Sie ganz einfach das Abbild der Statusaufnahme wiederherstellen.

IMAGEW.EXE ist mit LANDesks Abbildverarbeitungstool für DOS (IMAGE.EXE) kompatibel.

Beschränkungen

Für die Verwendung mit Windows 9x/Me setzt IMAGEW.EXE voraus, dass das System Int 13h-Erweiterungen unterstützt. Wenn Ihr Computer-BIOS aus irgendwelchen Gründen den Zugriff auf die Festplatte limitiert und kein Drive Manager zur Verfügung steht, um diese Beschränkung zu korrigieren, dann ist IMAGE.EXE auf diesen Betriebssystemen ebenfalls Beschränkungen unterworfen.

Systemvoraussetzungen

- IBM-kompatibler Personal Computer mit einem i80386-kompatiblen Mikroprozessor oder größer
- Windows 32-basierte Umgebung mit mindestens 32 MB RAM wird empfohlen
- Administratorrechte für die Ausführung unter Windows NT, Windows 2000 oder Windows XP

IMAGEW.EXE wird als Teil der LANDesk Betriebssystem-Verteilung im Verzeichnis \Program Files\LANDesk\ManagementSuite\osd\imaging installiert.

Erstellen von Abbildern

Sie können unterschiedliche Umgebungsvariablen und Befehlszeilenoptionen verwenden, um sicherzustellen, dass die erstellten Abbilder Ihre Anforderungen erfüllen.

Umgebungsvariablen

Die Umgebungsvariablen für IMAGEW.EXE müssen mit Befehlszeilenoptionen verwendet werden. Folgende Umgebungsvariablen stehen zur Verfügung:

- **IBXT** ändert die Methode, mit der ein Satz CDs gebrannt wird, sodass IMAGEW.EXE während einer Wiederherstellung nicht die letzte CD anfordert. Setzen Sie IBXT auf den Wert 1 (d.h., set ibxt=1). Diese Einstellung wird möglicherweise nicht von allen CD-R/RW-Laufwerken unterstützt.

- **IAR** ermöglicht es IMAGEW.EXE, beim Schreiben eines Abbilds in eine Datei automatisch auf Benutzereingaben und Fehlermeldung zu reagieren. Setzen Sie IAR auf Y oder N (d.h., set iar=Y). Mit dieser Einstellung werden alle 'Y'es- oder 'N'o-Eingabeaufforderungen, die das Betätigen der Eingabetaste durch den Benutzer erforderlich machen, automatisch beantwortet. Sie können DOS-Fehlerebenen in einer Stapeldatei verwenden, um festzustellen, ob der Vorgang erfolgreich war oder abgebrochen wurde.

Befehlszeilenoptionen

IMAGEW.EXE unterstützt die Verwendung von Befehlszeilenoptionen. Trennen Sie die Optionen durch Leerzeichen und geben Sie sie in der unten angegebenen Reihenfolge ein. Verwenden Sie die Befehlszeilenoption /? für zusätzliche Befehlszeilenoptionen, die hier nicht erläutert werden.

So erstellen Sie ein komprimiertes Abbild in einer Datei

Format 1: imagew /Ch# d:\filename.img (keine Validierung)

Format 2: imagew /Ch#V d:\filename.img (Validierung)

Format 3: imagew /Ch#VB d:\filename.img (Byte-für-Byte-Validierung)

Erläuterung: Ersetzen Sie das "h" durch die Nummer 0 bis 7 der Quellfestplatte und das # durch die Partitionseintrags-ID. Für die meisten Benutzer ist die Partitions-ID eine Zahl zwischen 1-4; für Datenträger ist sie eine Zahl, die als 0xPVV formatiert wurde, wobei P die erweiterte Partition und VV die Datenträgernummer im Hexadezimalformat von 01 bis FF ist.

Wenn Ihnen die Partitions- oder Datenträger-ID nicht bekannt ist, führen Sie IMAGEW.EXE ohne jegliche Befehlszeilenoptionen aus und wählen Sie "Abbild erstellen". Der Bildschirm, in dem die Partitionen und Datenträger aufgelistet werden, zeigt auch die ID in Klammern als eine Hexadezimalzahl an. Sie sollten dieser Zahl ein 0x in der Befehlszeile voranstellen.

So erstellen Sie ein nicht komprimiertes Abbild in einer Datei

Format 1: imagew /Ch# /U d:\filename.img (keine Validierung)

Format 2: imagew /Ch#V /U d:\filename.img (Validierung)

Format 3: imagew /Ch#VB /U d:\filename.img (Byte-für-Byte-Validierung)

Erläuterung: Wie oben.

So erstellen Sie ein komprimiertes Abbild in einem CD-Laufwerk

Format 1: imagew /Ch# /CDx

Erläuterung: Die Informationen bzgl. "h" und "#" sind dieselben wie weiter oben. Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x (/CD) aus, um eine Geräteliste zu erhalten.

So erstellen Sie ein nicht komprimiertes Abbild in einem CD-Laufwerk

Format 1: imagew /Ch# /U /CDx

Erläuterung: Wie oben.

So stellen Sie ein Abbild aus einer Datei wieder her

Format 1: imagew /R d:\filename.img (keine Validierung)

Format 2: imagew /RV d:\filename.img (Validierung nach Bedarf)

Erläuterung: Stellt das Abbild im selben Festplattenlaufwerk und im selben Speicherort wieder her, von dem aus das Abbild erstellt wurde.

So stellen Sie ein Abbild von einer CD wieder her

Format 1: imagew /R /CDx

Erläuterung: Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x aus, um eine Geräteliste zu erhalten.

So limitieren Sie die Dateigröße beim Erstellen

Format: d:\Dateiname;s

Erläuterung: Ersetzen Sie das "s" nach ";" durch 0 für 2 GB, 1 für 698 MB oder 2 für 648 MB.

Punkte zur Beachtung

- Für die Ausführung unter Windows NT/2000/XP Pro werden Administratorrechte benötigt. Unter Windows 2000/XP wird die Ausführung als beliebiger Benutzer unterstützt. Klicken Sie hierfür mit der rechten Maustaste und wählen Sie die Option "Ausführen als".
- Beim Erstellen eines Abbilds sollten Sie die Partition, von der die Sicherungskopie erstellt werden, nicht als Speicherort für die Abbilddatei verwenden. Falls Sie dies tun, wird die Partition zur selben Zeit aktualisiert wie versucht wird, eine Sicherungskopie von ihr zu erstellen. Dies hat zur Folge, dass sich das Dateisystem beim Wiederherstellen der Partition in einem nicht synchronisierten Zustand befindet.
- Wenn Sie eine Sicherung durchführen, ohne eine Sperrung angefordert zu haben, befindet sich die Sicherung möglicherweise nicht in einem synchronisierten Zustand, wenn das Laufwerk während des Sicherungsvorgangs aktualisiert wurde.
- Das Abbild kann nicht auf der Partition wiederhergestellt werden, in der sich die Quelldatei für das Abbild befindet. Wenn Sie dies tun, überschreibt die Wiederherstellung die Dateisystemstrukturen und die eigentliche Abbilddatei.
- Nach der Wiederherstellung muss das System möglicherweise neu gestartet werden. Dies ist unter bestimmten Bedingungen erforderlich und wird durch das Programm bestimmt. Wenn Sie trotz Aufforderung keinen Neustart ausführen, nimmt das Betriebssystem an, dass die Partition und das Dateisystem sich im selben Zustand befinden wie vor der Wiederherstellung. Dies kann Datenschäden verursachen. Sie können eine Befehlszeilenwiederherstellung mit /RN überschreiben. /RN sollte jedoch nur von versierten Benutzern verwendet werden, die wissen, dass die Nichtausführung des Neustarts kein Risiko darstellt.

- Beim Durchführen einer Befehlszeilenwiederherstellung wird die wiederhergestellte Partition auf dieselbe Festplattennummer und in dieselbe physikalische Speicherposition auf dem Laufwerk geschrieben, von der aus ihre Sicherungskopie erstellt wurde. Wenn dies ein Datenträger (Volume) war und es jetzt an dieser Speicherposition keine erweiterte Partition gibt, versucht die Wiederherstellung, die ursprüngliche erweiterte Partition zu erstellen. Wenn die erweiterte Partition nicht erstellt werden kann, wir sie als primäre Partition wiederhergestellt. Wenn die Position, von der aus die Partition gesichert wurde, eine primäre Partition war und dieser Stelle jetzt von einer erweiterten Partition belegt wird, wird sie als Datenträger (Volume) wiederhergestellt. Wenn eine vorhandene Partition oder ein Datenträger (Volume) an derselben Stelle beginnt wie die wiederherzustellende Partition, wird eine Warnmeldung eingeblendet, bevor die betreffende Partition oder das Volume überschrieben wird.
- Um den Wiederherstellungsprozess durch Starten der CD auszuführen, benötigen Sie ein ATAPI CD-Laufwerk. Für SCSI-Laufwerke müssen Sie Ihre eigene CDBOOT.F35-Datei erstellen, um die geeigneten DOS ASPI-Treiber zu laden und IMAGEW.EXE nach Bedarf über AUTOEXEC.BAT zu starten.

Hilfe zum Betriebssystem-Verteilung/Migrationstasks-Assistenten

In diesem Abschnitt werden die Optionen und Einstellungen beschrieben, die auf den einzelnen Seiten (und Dialogfeldern) des Betriebssystem-Verteilung/Migrationstasks-Assistenten verfügbar sind. Dieser Assistent dient zum Erstellen von Skripts, mit denen OS-Abbilder erfasst oder bereitgestellt und Benutzerprofile erfasst oder wiederhergestellt werden. Skripts können als Task auf Ziel-Clients im Netzwerk eingeplant werden. Der Assistent wird entweder über die betreffende Symbolleistenschaltfläche oder die Kontextmenüs im Fenster "Skripte verwalten" (**Extras | Skripte verwalten**) aufgerufen.

Sie können auf diese Informationen auch zugreifen, indem Sie auf der betreffenden Seite des Assistenten auf die Schaltfläche "Hilfe" klicken.

Detaillierte Schritt-für-Schritt-Anleitungen zur Verwendung des Betriebssystem-Verteilung/Migrationstasks-Assistenten und zur Planung und Implementierung von Abbildbereitstellungs- und Migrationsaufträgen finden Sie in Kapitel 9 "Verteilen von Betriebssystemabbildern und Migrieren von Profilen".

Hinweis: Hier werden sämtliche Seiten des Betriebssystem-Verteilung/Migrationstasks-Assistenten beschrieben. Welche Seiten während der Ausführung des Assistenten tatsächlich angezeigt werden, hängt allerdings von dem Typ des Abbildungs- oder Migrationstask ab, den Sie auf der ersten Seite des Assistenten auswählen.

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Wählen Sie einen Task"

Auf dieser Seite geben Sie anhand der folgenden Tasks an, welche Art von Betriebssystem-Verteilung/Profilmigrationsskript erstellt werden soll:

- **Abbild erfassen:** Erstellt ein Skript, das ein Betriebssystemabbild von einem Client erfasst und speichert. Abbilder können mit dem integrierten LANDesk-Abbildverarbeitungstool, das zusammen mit Management Suite installiert wird, oder mit einem Tool eines Fremdherstellers, wie z. B. Ghost* oder PowerQuest*, oder einem anderen Tool Ihrer Wahl erfasst werden.
- **Profil erfassen:** Erstellt ein Skript, das die einem Client eigenen Benutzereinstellungen, Anwendungs- und Desktopeinstellungen sowie Dateien erfasst. Sie können über diese Option auch auf das Dialogfeld "Sammlungsmanager" zugreifen, um ein benutzerinitiiertes Profilmigrationspaket zu erstellen, das auf einzelnen Clients lokal ausgeführt werden kann.
- **Abbild bereitstellen:** Erstellt ein Skript, das ein zuvor erfasstes OS-Abbild für Ziel-Clients bereitstellt.
- **Abbild bereitstellen (mit Profilerfassung und -wiederherstellung):** Erstellt ein Skript, das einen umfassenden Bereitstellungs- und Migrationsauftrag ausführt (Erfassen von Profildaten, Bereitstellen eines Betriebssystem-Abbilds und Wiederherstellen des Profils).
- **Profil wiederherstellen:** Erstellt ein Skript, das zuvor erfasste Profildaten auf Ziel-Clients wiederherstellt (Benutzereinstellungen, Anwendungs- und Desktopeinstellungen sowie Dateien).
- **Generische DOS-Tasks:** Erstellt ein Skript, das auf Clients DOS-Befehle ausführt (einschließlich Starten von Anwendungen).

Verwandte Themen

- Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Erstellen von Migrationsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Übersicht über die Betriebssystem-Verteilung
- Übersicht über die Profilmigration

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Bildverarbeitungs-Task konfigurieren"

Auf dieser Seite konfigurieren Sie die folgenden Merkmale eines Betriebssystem-Bildverarbeitungs-Task:

Hinweis: Einige der unten aufgeführten Optionen sind, abhängig von dem auf der ersten Seite des Assistenten gewählten Tasktyp (Erfassen oder Bereitstellen), möglicherweise deaktiviert.

- **Multicast verwenden:** Einsatz bestehender Multicast-Domänenrepräsentanten in Subnetzen Ihres Netzwerks, um das Betriebssystemabbild mithilfe der Targeted Multicasting-Technologie von LANDesk bereitzustellen. Die Targeted Multicasting-Technologie ermöglicht es Ihnen, Softwarepakete gleichzeitig an mehrere Clients zu übermitteln, wodurch der erforderliche Zeit- und Bandbreitenaufwand beträchtlich verringert wird. Statt für jeden Client ein Paket über das Netzwerk zu senden, wird für jedes Subnetz nur eine Übertragung durchgeführt.

  Hinweis: Bevor Sie die Targeting Multicasting-Technologie einsetzen, müssen Sie sicherstellen, dass die Targeted Multicasting-Komponenten in dem Subnetz vorhanden sind, an das Pakete verteilt werden. Für Targeted Multicasting sind Agenten von Management Suite 6.62 oder höher und ein Multicast-Domänenrepräsentant der Version 6.62 oder höher erforderlich.

- **Abbild ist mit SysPrep vorbereitet:** Diese Option zeigt an, dass Sie das bereitzustellende Betriebssystem-Abbild mit Microsoft SysPrep konfiguriert haben. Wenn Sie diese Option auswählen, können Sie auf einer nachfolgenden Seite des Assistenten SysPrep-Dateiinformationen und -Bereitstellungsoptionen angeben.
- **Profilmigration einbeziehen:** Bindet sowohl Profilerfassungs- als auch -wiederherstellungsprozesse in den Abbildbereitstellungsauftrag ein. Wenn Sie diese Option auswählen, können Sie auf einer nachfolgenden Seite des Assistenten Profilmigrationsoptionen angeben.
- **Wählen Sie den zu verwendenden Netzwerkadapter, wenn die automatische Treibererkennung fehlschlägt:** Mit dieser Option wird sichergestellt, dass der Abbildbereitstellungsauftrag auf allen Ziel-Clients erfolgreich ausgeführt werden kann. Wir empfehlen, dass Sie diese Option aktivieren und dann einen Netzwerkadapter auswählen, der in Ihren Systemen gängig ist. Dies ist insbesondere dann wichtig, wenn Laptop-Computer die Ziel-Clients sind. Sie sollten sorgfältig vorgehen und einen der aufgeführten Netzwerkadapter auswählen, um die erfolgreiche Ausführung des Auftrags zu gewährleisten.

  Die Netzwerkadaptererkennung durch die Betriebssystem-Verteilung erfolgt in mehreren Stufen.

  - Zuerst versucht die Betriebssystem-Verteilung, den Netzwerkadapter im Betriebssystem des Ziel-Clients zu erkennen, bevor dieser durch das Abbild überschrieben wird.
  - Falls dies fehlschlägt, startet die Betriebssystem-Verteilung den Ziel-Client neu und versucht, den Netzwerkadapter unter DOS zu erkennen.
  - Falls dies fehlschlägt, verwendet die Betriebssystem-Verteilung den Netzwerkadapter, den Sie unter der Option "Nicht erkennbare Netzwerkadapter" auf dieser Seite des Assistenten angegeben haben.
  - Falls der von Ihnen angegebene Adapter nicht funktioniert, müssen Sie zum Ziel-Client gehen und diesen von Hand neu starten. Der Client wird normalerweise mit seinem ursprünglichen Betriebssystem hochgefahren.

Verwandte Themen

- Multicasting für Betriebssystemabbilder
- Richtlinien für Betriebssystemabbilder
- Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Übersicht über die Betriebssystem-Verteilung
- Übersicht über die Profilmigration

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Skriptdaten eingeben"

Auf dieser Seite bezeichnen Sie das Betriebssystem-Verteilung- und Profilmigrationsskript. Der hier eingegebene Text wird verwendet, wenn das Skript in den Fenstern "Skripte verwalten" und "Geplante Tasks" angezeigt wird.

- **Skriptname:** Bezeichnung des Skripts durch einen eindeutigen Namen. Falls der hier eingegebene Name bereits verwendet wird, werden Sie aufgefordert zu bestätigen, dass das vorhandene Skript ersetzt werden soll. Sie sollten einen Namen eingeben, der es Ihnen erleichtert, das Skript anhand seiner Funktion oder der vorgesehenen Ziel-Clients in Ihrem Netzwerk rasch und mühelos zu identifizieren.
- **Skriptbeschreibung:** (Optional) Der hier eingegebene Text dient als Gedächtnisstütze bei der Identifizierung des Skripts.

> **Hinweis:** Wenn Sie dieses Skript dem LANDesk PXE-DOS-Menü hinzufügen, wird die hier eingegebene Beschreibung im Menü angezeigt.

Verwandte Themen

- Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Übersicht über die Betriebssystem-Verteilung
- Übersicht über die Profilmigration
- Konfigurieren des LANDesk PXE DOS- (Start-) Menüs

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Geben Sie Berechtigungsnachweise für die Freigabe des Abbildes und Abbildverarbeitungstools ein"

Auf dieser Seite stellen Sie Berechtigungsnachweise für den oder die freigegebenen Netzwerkordner bereit, in dem bzw. denen das Betriebssystem-Abbild und das Abbildverarbeitungstool, mit dem das Abbild erstellt wurde, gespeichert sind.

Hinweis: Sie können lediglich einen Satz von Berechtigungsnachweisen eingeben, der für den Zugriff auf beide Freigaben verwendet wird; daher müssen die Berechtigungsnachweise für diese Freigaben übereinstimmen. Die Berechtigungsnachweise müssen einem lokalen Benutzerkonto auf dem Client gehören, der die Freigabe beherbergt.

- **Benutzername:** Angabe eines Benutzerkontos, das über die Berechtigungsnachweise verfügt, die für die Anmeldung bei der Netzwerkfreigabe erforderlich sind.
- **Kennwort:** Kennwort des Benutzers.
- **Domäne:** Active Directory-Domäne des Benutzers.

Verwandte Themen

- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Wählen Sie den Abbildspeicherort und das Abbildverarbeitungstool"

Auf dieser Seite geben Sie an, welcher Typ von Abbild mit diesem Skript erfasst werden soll, wo das Abbild gespeichert werden soll und an welchem Speicherort sich das Abbildverarbeitungstool befindet.

- **Abbildtyp:** Bezeichnung des Dateityps (Formats) der Abbilddatei, die mit diesem Skript erfasst wird; der Dateityp wird durch die Auswahl eines Tools aus der Liste der Abbildverarbeitungstools festgelegt.
- **UNC-Pfad zum Speicherort des neuen Abbildes:** Bezeichnung des Servers und der Freigabe, die als Speicherort der Abbilddatei dienen sollen. Das Abbild muss in einem freigegebenen Ordner gespeichert werden, auf den Clients zugreifen können. Beachten Sie, dass der Freigabename keine Leerzeichen enthalten darf. Sie können den Clientnamen einfach im UNC-Format angeben und dann die restliche Pfadangabe ergänzen, indem Sie auf die Schaltfläche "Durchsuchen" klicken und die Freigabe suchen.

  > **Hinweis:** Während des Abbildverarbeitungsprozesses ordnen Clients dem Abbildspeicherort das Laufwerk I: zu.

- **UNC-Pfad zum Abbildverarbeitungstool:** Bezeichnung des Servers und der Freigabe, die den Speicherort des Abbildverarbeitungstools (das dem oben gewählten Abbildtyp entspricht) bilden, einschließlich des Namens der .EXE-Datei des Tools. Beachten Sie, dass der Freigabename keine Leerzeichen enthalten darf.

  > **Hinweis:** Während des Abbildverarbeitungsprozesses ordnen Clients diesem UNC-Pfad das Laufwerk H: zu.

Verwandte Themen

- Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Übersicht über die Betriebssystem-Verteilung
- Übersicht über die Profilmigration

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Abbild zur Wiederherstellung auf Ziel-Clients auswählen"

Auf dieser Seite geben Sie an, welcher Typ von Abbild mit diesem Skript wiederhergestellt werden soll, wo das Abbild gespeichert ist und an welchem Speicherort sich das Abbildverarbeitungstool befindet.

- **Abbildtyp:** Bezeichnung des Dateityps (Formats) der vorhandenen Abbilddatei, die durch dieses Skript bereitgestellt werden soll; der Dateityp wird durch die Auswahl eines Tools aus der Liste der Abbildverarbeitungstools festgelegt.
- **UNC-Pfad zur wiederherzustellenden Abbilddatei:** Bezeichnung des Servers und der Freigabe, die als Speicherort der Abbilddatei dienen, einschließlich des Abbilddateinamens. Das Abbild muss in einem freigegebenen Ordner gespeichert werden, auf den Clients zugreifen können.
- **UNC-Pfad zum Abbildverarbeitungstool:** Bezeichnung des Servers und der Freigabe, die den Speicherort des Abbildverarbeitungstools (das dem oben gewählten Abbildtyp entspricht) bilden, einschließlich des Namens der .EXE-Datei des Tools.

Verwandte Themen

- Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Übersicht über die Betriebssystem-Verteilung
- Übersicht über die Profilmigration

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Zusätzliche Bereitstellungsbefehle eingeben"

Auf dieser Seite können Sie das Skript anpassen, indem Sie DOS-Befehle, Befehlszeilenparameter für das Abbildverarbeitungstool und "RunOnce"-Befehle hinzufügen.

Hinweis: Die Option zur Eingabe von "RunOnce"-Befehlen wird nur angezeigt, wenn Sie ein Skript für die Abbildbereitstellung erstellen, jedoch nicht bei der Erstellung eines Skripts für die Abbilderfassung.

- **Geben Sie Befehle ein, die vor dem Neustart und der Abbilderstellung des Clients ausgeführt werden sollen:** Angabe von DOS-Befehlen oder Windows-Programmen. Sie können diesem Textfeld Befehle hinzufügen, wobei Sie diese wie an der DOS-Eingabeaufforderung jeweils in einer eigenen Zeile eingeben müssen. Die einzelnen Befehle werden nacheinander an Clients geschickt.

  Hinweis: Nachdem die Ausführung dieser Befehle abgeschlossen worden ist, wird das Betriebssystem heruntergefahren und der Client mit seiner virtuellen Boot-Partition neu gestartet.

- **Geben Sie zusätzliche Befehlszeilenparameter für das Abbildverarbeitungstool ein:** Angabe zusätzlicher Befehlszeilenparameter für das gewählte Abbildverarbeitungstool. Sie können in diesem Textfeld am Ende der Standardbefehlszeile Parameter hinzufügen. Nähere Informationen zu den zulässigen Befehlszeilenparametern finden Sie in der Dokumentation zu Ihrem Abbildverarbeitungstool.
- **Geben Sie die Befehle 'RunOnce' ein, die ausgeführt werden, nachdem das Setup SYSPREP auf dem Client ausgeführt wurde:** (Diese Option betrifft lediglich Skripts für die Abbildbereitstellung) Angabe von Befehlen zum Start von Anwendungsprogrammen, die Windows ausführen soll, nachdem der Client (nach der Beendigung von SysPrep) zum ersten Mal gestartet wurde. Sie können diesem Textfeld Befehle hinzufügen, wobei Sie diese wie an der DOS-Eingabeaufforderung jeweils in einer eigenen Zeile eingeben müssen.

  Hinweis: Diese Befehle werden dem Windows-Registrierungsschlüssel RunOnce hinzugefügt: \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

- **Fertigstellen:** Speichern des Skripts für die Abbildbereitstellung und Beenden des Assistenten.
- **Abbrechen:** Beenden des Assistenten, ohne das Skript zu speichern.

Verwandte Themen

- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Multicast-Optionen konfigurieren"

Auf dieser Seite konfigurieren Sie die folgenden grundlegenden LANDesk Targeted Multicasting-Optionen für ein Abbildbereitstellungsskript:

- **Multicast-Domänenerkennung verwenden:** Bevor die Targeted Multicasting-Technologie eingesetzt wird, um das Abbild an Clients im Netzwerk zu verteilen, wird in Subnetzen Ihres Netzwerks nach Multicast-Domänenrepräsentanten gesucht.
- **Multicast-Domänenerkennung verwenden und Ergebnisse speichern:**Vor der Bereitstellung des Abbilds wird in Subnetzen Ihres Netzwerks nach Multicast-Domänenrepräsentanten gesucht, und die Ergebnisdaten werden gespeichert, um künftige Targeted Multicasting-Bereitstellungen zu erleichtern.

  Es werden jeweils nur die Ergebnisse eines Suchlaufs der Multicast-Domänenerkennung gespeichert; wenn Sie diese Option für ein Abbildbereitstellungsskript auswählen, werden daher die Ergebnisse der vorherigen Multicast-Domänenerkennung überschrieben.

- **Ergebnisse der letzten Multicast-Domänenerkennung verwenden:** Beim Verteilen des Abbilds an Clients wird die zuletzt erstellte Liste erkannter Multicast-Domänenrepräsentanten verwendet.

  Hinweis: Wählen Sie diese Option NUR dann aus, wenn Sie die Ergebnisdaten einer Multicast-Domänenerkennung schon mindestens einmal gespeichert haben.

- **Erweiterte Multicast-Optionen konfigurieren:** Ermöglicht Ihnen eine weitergehende Anpassung der Targeted Multicasting-Funktion für ein Bereitstellungsskript, indem Sie auf der nächsten Seite des Assistenten erweiterte Multicast-Optionen konfigurieren.

Verwandte Themen

- Multicasting für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Erweiterte Multicast-Optionen konfigurieren"

Auf dieser Seite konfigurieren Sie die folgenden erweiterten LANDesk Targeted Multicasting-Optionen für ein Abbildbereitstellungsskript:

- **Höchstzahl gleichzeitig arbeitender Multicast-Domänenrepräsentanten:** Bestimmt die Höchstzahl von Multicast-Domänenrepräsentanten, die gleichzeitig unter Verwendung der Targeted Multicasting-Technologie ein Abbild aktiv bereitstellen können.
- **Anzahl von Tagen, die die Dateien im Cache des Client verbleiben:** Legt die Zeitspanne fest, über die das per Multicasting bereitgestellte Abbild im lokalen Cache der einzelnen Ziel-Clients verbleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Anzahl der Tage, die Dateien im Multicast-Domänenrepräsentanten-Cache bleiben:** Legt die Zeitspanne fest, über die das per Multicasting bereitgestellte Abbild im Cache der Multicast-Domänenrepräsentanten verbleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Mindestanzahl der Millisekunden zwischen Paketübertragungen:** Bestimmt die Zeitspanne, die zwischen einzelnen Sendungen von Multicast-Paketen mindestens abgewartet werden muss. Dieser Wert wird nur verwendet, wenn der Multicast-Domänenrepräsentant keine Datei aus seinem eigenen Cache per Multicast übermittelt. Sie können mithilfe dieses Parameters die Bandbreitennutzung im WAN beschränken.

  Hinweis: Wird dieser Parameter nicht angegeben, dann wird die voreingestellte Mindestzeit für den Ruhezustand, die im Multicast-Domänenrepräsentanten des Subnetzes gespeichert ist, eingesetzt.

- **Maximale Anzahl der Millisekunden zwischen Paketübertragungen:** Bestimmt die maximale Zeitspanne, die zwischen einzelnen Sendungen von Multicast-Paketen abgewartet werden muss.

Verwandte Themen

- Multicasting für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Sysprep-Dateiinformationen angeben"

Auf dieser Seite geben Sie die folgenden Informationen zur Sysprep-Datei (SYSPREP.INF) an, die von diesem Skript verwendet wird, um das bereitzustellende Abbild zu modifizieren:

- **SYSPREP.INF-Dateiquelle - Vorhandene SYSPREP.INF-Datei als Vorlage verwenden:** Eine vorhandene SYSPREP.INF-Datei wird als Vorlage für eine neue Datei verwendet, und hier wird der Speicherort der vorhandenen Datei angegeben. Die neue SYSPREP.INF-Datei, die die in diesem Assistenten vorgenommenen Einstellungen enthält, überschreibt die vorhandene Sysprep-Standarddatei. Wenn OSD die SYSPREP.INF-Datei auf der Grundlage einer von Ihnen erstellten Datei anlegen soll, dann können Sie nach dieser Datei suchen. Falls Sie keine vorhandene SYSPREP.INF-Datei auswählen, erstellt OSD eine neue Datei.

  Hinweis: Nach der Fertigstellung des Assistenten können Sie die mit einem Skript verknüpfte SYSPREP.INF-Datei bearbeiten, indem Sie mit der rechten Maustaste auf das Skript klicken und anschließend auf **Erweiterte Bearbeitung** klicken.

- **SYSPREP.INF-Speicherort des bereitgestellten Abbildes:** Angabe des Speicherorts, an dem sich die Datei SYSPREP.INF auf der Festplatte des Clients befand, auf dem Sysprep ursprünglich ausgeführt wurde. Mit anderen Worten, der Client, dessen Abbild durch dieses Skript bereitgestellt wird.
- **SYSPREP.INF-Multiprozessorabbildunterstützung - Erweiterte Multiprozessoroptionen konfigurieren:**Diese Option ermöglicht es Ihnen, auf der nächsten Seite des Assistenten ein Abbild zu konfigurieren, das Multiprozessorsysteme (bei Clients unter Windows 2000 oder Windows XP) unterstützt.

  Hinweis: Wählen Sie diese Option nur dann aus, wenn sich die Prozessoranzahl im Abbild von der Prozessoranzahl eines Ziel-Clients unterscheidet.

Verwandte Themen

- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Multiprozessordaten konfigurieren"

Auf dieser Seite konfigurieren Sie die folgenden Multiprozessor-Einstellungen für das Abbild, das durch dieses Skript bereitgestellt wird:

- **Geben Sie den Betriebssystemtyp für das auf den Zielcomputern bereitgestellte Abbild ein:** Angabe des Betriebssystems, das Bestandteil des bereitgestellten Abbilds ist; dies ist entweder Windows 2000 oder Windows XP.
- **Auf welchem Computertyp wurde das Abbild erstellt:** Angabe, ob das bereitzustellende Abbild auf einem Einprozessor- oder einem Multiprozessor-Client mit APIC oder MPS-Architektur erzeugt wurde.
- **Geben Sie den Ort der HAL-bezogenen .INF-Dateien im Abbild ein:** Angabe des Pfads der HAL-bezogenen .INF-Datei für das Abbild, das durch dieses Skript bereitgestellt wird. Per Voreinstellung verwendet der Assistent für jedes Betriebssystem die von Microsoft definierten .INF-Standarddateipfade. Wenn Sie bei der Konfiguration des Clients für die Abbilderstellung die Standardpfade verwendet haben, behalten Sie die Angaben in diesem Textfeld bei. Andernfalls geben Sie den Pfad ein, den Sie für die HAL-bezogene .INF-Datei benutzt haben.

Zusätzliche Multiprozessordaten

Einprozessor- und Multiprozessor-Clients erfordern verschiedene Windows 2000- und Windows XP-Kernel. Abhängig von der Hardwarekonfiguration, können Sie möglicherweise ein für ein Einprozessorsystem erstelltes Abbild auch auf einem Multiprozessor-Client verwenden oder umgekehrt.

Clients, die erweiterte Prozessorfunktionen unterstützen, verfügen in der Regel über einen Controller vom Typ APIC (Advanced Programmable Interrupt Controller). Clients, die erweiterte Prozessorfunktionen unterstützen, können zudem mit einer ACPI- (Advanced Configuration and Power Interface-) Schnittstelle ausgestattet sein.

Die Bedingungen, unter denen ein Abbild sowohl für Einprozessor- als auch Multiprozessor-Clients verwendet werden kann, sind kompliziert. Detaillierte Informationen hierzu finden Sie in der Sysprep-Dokumentation von Microsoft.

WARNUNG: Grundsätzlich ist bei der gemeinsamen Nutzung von Einprozessor- und Multiprozessorabbildern zu beachten, dass sowohl Quell- als auch Ziel-Clients entweder eine APIC-HAL mit ACPI-Unterstützung oder eine APIC-HAL ohne ACPI-Unterstützung besitzen müssen. Sie können auf einem APIC-Client ohne ACPI-Unterstützung kein ACPI-APIC-Abbild verwenden und umgekehrt auf einem ACPI-APIC-Client kein APIC-Abbild ohne ACPI-Unterstützung.

Verwandte Themen

- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Generische Sysprep-Optionen angeben"

Auf dieser Seite geben Sie die folgenden allgemeinen Einstellungen für die Datei SYSPREP.INF an, die von diesem Skript verwendet wird, um das bereitzustellende Abbild zu modifizieren:

- **Zeitzone:** Angabe der Zeitzone, in der sich die Ziel-Clients befinden.
- **Datenträgerlizenzschlüssel:** Angabe der Lizenznummer des Betriebssystems, das bereitgestellt wird.
- **Lokales Administratorkennwort für dieses Abbild:** Angabe des Administratorkennworts für den Client, auf dem das Abbild erstellt wurde.
- **Name:** Bezeichnung der Ziel-Clients durch einen Namen, wie den Namen einer Abteilung oder eines geografischen Standorts.
- **Organisation:** Bezeichnung der Organisation durch einen Namen, z. B. den Namen eines Geschäftsbereichs oder einen Firmennamen.

Verwandte Themen

- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Sysprep-Netzwerkoptionen angeben"

Auf dieser Seite legen Sie die folgenden Netzwerkeinstellungen fest, die in die SYSPREP.INF-Datei dieses Abbilds aufgenommen werden sollen:

- **Arbeitsgruppe:** Angabe, dass die Ziel-Clients Mitglieder einer Arbeitsgruppe sind. Wenn Sie diese Option auswählen, müssen Sie den Namen der Arbeitsgruppe in das Textfeld eingeben.
- **Domäne:** Angabe, dass die Ziel-Clients Mitglieder einer Domäne sind. Wenn Sie diese Option auswählen, müssen Sie den Namen der Domäne in das Textfeld eingeben und die folgenden Informationen zu Domänenkonten bereitstellen:
  - **Benutzername:** Name eines Domänenbenutzers, der zum Hinzufügen eines Rechnerkontos zu dieser Domäne berechtigt ist.
  - **Kennwort:** Stellt das Kennwort des Benutzers zur Verfügung.
  - **Rechner zu Organisationseinheit hinzufügen:** Angabe des Pfads (unter Verwendung der LDAP-Pfadsyntax) einer bestimmten Microsoft Active Directory-Organisationseinheit, zu der die abzubildenden Ziel-Clients hinzugefügt werden sollen.

Verwandte Themen

- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Namenskonvention für Zielcomputer zuweisen"

Auf dieser Seite weisen Sie die Namenskonvention für die Ziel-Clients zu, die durch das Abbildbereitstellungsskript abgebildet werden.

- **Erst versuchen, vorhandene Computernamen aus der Inventardatenbank abzurufen und zu verwenden:** Mit dieser Option werden vorhandene Windows-Computernamen beibehalten, falls die Ziel-Clients bereits vom Inventarscanner erfasst wurden. Das Abbild versucht dann, bereits in der Core-Datenbank vorhandene Computernamen zu verwenden.
- **Verwenden Sie falls notwendig die folgende Vorlage zur Benennung der Zielcomputer:** Angabe einer Vorlage, die eine Namenskonvention zur Erzeugung eindeutiger Namen für diejenigen Ziel-Clients definiert, denen in der Core-Datenbank aktuell noch kein Gerätename zugeordnet ist. Diese Vorlage ist nützlich für Clients, die von der CBA-Erkennung ermittelt werden oder über PXE-Startoptionen verfügen. Siehe Beispiele auf der betreffenden Seite des Assistenten.

Verwandte Themen

- Erstellen benutzerdefinierter Computernamen
- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Geben Sie Informationen für den Installationsort des LANDesk Management Suite-Client ein"

Auf dieser Seite geben Sie die folgenden Informationen ein, die im Abbild zur Installation der LANDesk-Clientsoftware auf den Ziel-Clients vorhanden sein müssen.

- **UNC-Pfad zum Verzeichnis, das WSCFG32.EXE enthält:** Angabe des UNC-Pfads (normalerweise \\<corename>\LDLogon) zum Core Server oder Service Center, in dem WSCFG32.EXE (die Clientsetup-Datei für Management Suite) gespeichert ist.
- **Berechtigungsnachweise für die Authentifizierung:** Angabe eines Benutzernamens, Kennworts und einer Domäne zur Authentifizierung beim Core Server oder Service Center, damit das Abbild die Datei WSCFG32.EXE auf den Ziel-Clients installieren kann.

Verwandte Themen

- Richtlinien für Betriebssystemabbilder
- Übersicht über die Betriebssystem-Verteilung

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Sammlung für dieses Profil auswählen"

Sie verwenden diese Seite, um eine Regelsammlung für das Profilmigrationsskript auszuwählen und um das Dialogfeld "Sammlungsmanager" zu öffnen. Eine Sammlung bestimmt den Profilinhalt, der vom Migrationsskript migriert (erfasst oder wiederhergestellt) werden soll:

- **Verfügbare Sammlungen:** Liste aller auf dem Core Server verfügbaren Sammlungen. Bei einer Sammlung handelt es sich um eine benutzerdefinierte Regelmenge, wobei jede Regel eine bestimmte Anwendung, Desktopeinstellung oder Datei bezeichnet, die migriert werden kann. Wenn Sie eine Sammlung in der Liste hervorheben, wird in dem darunter liegenden Meldungsfeld eine Beschreibung dieser Sammlung angezeigt.

  > **Hinweis:** Sie können für jedes Migrationsskript nur jeweils eine Sammlung auswählen. Allerdings können Sie beliebig viele Sammlungen erstellen und bearbeiten, die verschiedene Kombinationen von Anwendungs-, Desktop- und Dateiregeln umfassen.

- **Verwalten:** Mit dieser Option greifen Sie auf das Dialogfeld "Sammlungsmanager" zu, in dem Sie Sammlungen und Dateiregeln definieren und bearbeiten sowie benutzerinitiierte Migrationspakete erstellen können.

Verwandte Themen

- Übersicht über die Profilmigration
- Profilinhalt
- Informationen zum Dialogfeld "Sammlungsmanager"

Informationen zum Dialogfeld "Sammlungsmanager"

In diesem Dialogfeld können Sie Regelsammlungen sowie einzelne Dateiregeln erstellen, bearbeiten und löschen. Sie können dieses Dialogfeld zudem zum Erstellen und Löschen benutzerinitiierter Profilmigrationspakete verwenden.

(Das Dialogfeld "Sammlungsmanager" kann entweder aus dem Betriebssystem-Verteilung/Migrationstasks-Assistenten heraus oder direkt über die Symbolleiste "Skripte verwalten" der Konsole aufgerufen werden.)

- **Dateiregeln:** Anzeige aller verfügbaren Dateiregeln im Listenfeld. Sie können eine neue Dateiregel definieren und eine vorhandene Regel bearbeiten.

  > **Hinweis:** Wenn Sie eine Dateiregel löschen, wird diese Regel vom Core Server entfernt. Jede Sammlung, die diese Regel enthielt, weist auf diese Änderung hin, wenn Sie die Sammlung das nächste Mal öffnen oder bearbeiten.

- **Sammlungen:** Anzeige aller verfügbaren Sammlungen im Listenfeld. Sie können eine neue Sammlung definieren und eine vorhandene Sammlung bearbeiten.

> **Hinweis:** Wenn Sie eine Sammlung löschen, wird diese Sammlung vom Core Server entfernt. Migrationsskripts, die auf diese Sammlung Bezug nehmen, werden nicht ordnungsgemäß ausgeführt. Sie sollten auch das betreffende Skript löschen.

- **Benutzerinitiiertes Paket:** Anzeige aller verfügbaren Pakete im Listenfeld. Sie können ein neues Migrationspaket erstellen, wobei es sich um eine selbstextrahierende ausführbare Datei handelt, die auf einzelnen Clients ausgeführt werden kann. Vorhandene benutzerinitiierte Pakete können nicht bearbeitet werden.

> **Hinweis:** Wenn Sie ein benutzerinitiiertes Paket löschen, wird dieses Paket vom Core Server entfernt. Abhängig davon, wie und wo Sie das Paket an Benutzer verteilt haben, können möglicherweise noch andere Kopien des Pakets vorhanden sein.

Verwandte Themen

- Erstellen von Dateiregeln
- Erstellen von Sammlungen
- Erstellen von benutzerinitiierten Migrationspaketen
- Übersicht über die Profilmigration
- Profilinhalt

Informationen zum Dialogfeld "Dateiregel"

In diesem Dialogfeld können Sie neue Dateiregeln erstellen und vorhandene bearbeiten (klicken Sie im Dialogfeld "Sammlungsmanager" auf **Dateiregeln** und anschließend auf **Neu**).

Eine Dateiregel legt anhand folgender Kriterien fest, welche Dateien migriert werden: Speicherort von Laufwerk und Verzeichnis, Unterverzeichnisse, Dateibenennung (einschließlich Verwendung von Platzhaltern) und Zielspeicherort.

- **Regelname:** Bezeichnung der Dateiregel durch einen eindeutigen Namen. Wenn Sie den Namen einer vorhandenen Dateiregel eingeben, werden Sie gefragt, ob diese überschrieben werden soll. Verwenden Sie einen Namen, der etwas über den Zweck und den Inhalt der Dateiregel aussagt.
- **Regelbeschreibung:** (Optional) Der hier eingegebene Text dient als Gedächtnisstütze bei der Identifizierung der Dateiregel.
- **Quellverzeichnis:** Angabe von Laufwerk und Verzeichnispfad des Speicherorts der Dateien, die Sie migrieren möchten.

Hinweis zu Festplattenpartitionen: Dateien können von den in einen Client fest eingebauten Laufwerken, einschließlich Festplattenpartitionen, migriert werden. Wechselmedien, wie z. B. CD-ROM-Laufwerke, und Netzwerkfreigaben werden nicht unterstützt. Falls der Ziel-Client nicht über einen entsprechenden Laufwerksbuchstaben für die Festplattenpartition verfügt, wird im Stammverzeichnis des Laufwerks C des Clients ein neues Verzeichnis namens "Migrated_[Laufwerksbuchstabe]_Drive" angelegt, und die Dateien werden (zusammen mit der zugehörigen Verzeichnisstruktur) in dieses neue Verzeichnis migriert.

- **Mit Unterverzeichnissen:** Alle Unterverzeichnisse des angegebenen Quellverzeichnisses werden nach Dateien durchsucht.
- **Zielverzeichnis zuweisen:** Die Dateien werden auf dem Ziel-Client in einen Pfad verschoben, der sich vom Quellverzeichnispfad unterscheidet. Die zu einer Datei gehörige Verzeichnisstruktur wird im neu zugewiesenen Pfad beibehalten.
- **Zielverzeichnis:** Angabe von Laufwerk und Verzeichnispfad auf dem Ziel-Client, wohin Dateien, die den Kriterien für Speicherort und Benennung entsprechen, migriert werden sollen.
- **Dateien berücksichtigen:** Angabe der Dateinamenssyntax, nach der Dateien im angegebenen Quellverzeichnis erfasst werden sollen. Sie können genaue Dateinamen angeben, wenn nur einzelne Dateien berücksichtigt werden sollen. Zudem ist die Angabe von Platzhalterzeichen (* und ?) zulässig, um Dateien auszuwählen, die einen bestimmten Dateityp bzw. eine bestimmte Erweiterung (z. B. *.txt), ein bestimmtes Präfix (z. B. meinName.*) oder ein anderes, mithilfe dieser Platzhalter beschriebenes Namensmuster besitzen.

  Hinweis: Sie können mehrere Dateinamen durch ein Semikolon (;) voneinander getrennt angeben.

- **Auszuschließende Dateien:** Angabe der Dateinamenssyntax für Dateien, die im angegebenen Quellverzeichnis nicht erfasst werden sollen. Sie können genaue Dateinamen angeben, wenn nur einzelne Dateien ausgeschlossen werden sollen. Zudem ist die Angabe von Platzhalterzeichen (* und ?) zulässig, um Dateien auszuschließen, die einen bestimmten Dateityp bzw. eine bestimmte Erweiterung (z. B. *.txt), ein bestimmtes Präfix (z. B. meinName.*) oder ein anderes, mithilfe dieser Platzhalter beschriebenes Namensmuster besitzen.

  Hinweis: Falls die Angaben der zu berücksichtigenden Dateien und der auszuschließenden Dateien einander widersprechen, dann hat die Angabe der auszuschließenden Dateien Vorrang und die betreffende(n) Datei(en) werden von der Dateiregel nicht erfasst.

Verwandte Themen

- Migrieren von Dateien und Ordnern
- Profilinhalt
- Übersicht über die Profilmigration

Informationen zum Dialogfeld "Regelsammlung"

In diesem Dialogfeld können Sie neue Sammlungen erstellen und vorhandene bearbeiten (klicken Sie im Dialogfeld "Sammlungsmanager" auf **Sammlungen** und anschließend auf **Neu**).

Eine Sammlung ist eine benutzerdefinierte Menge von Anwendungs-, Desktop- und Dateiregeln, die den zu migrierenden Profilinhalt festlegt.

- **Sammlungsname:** Bezeichnung der Sammlung durch einen eindeutigen Namen. Wenn Sie den Namen einer vorhandenen Sammlung eingeben, werden Sie gefragt, ob diese überschrieben werden soll. Verwenden Sie einen Namen, der etwas über den Zweck und den Inhalt der Sammlung aussagt.
- **Beschreibung:** (Optional) Der hier eingegebene Text dient als Gedächtnisstütze bei der Identifizierung der Sammlung. Die hier eingegebene Beschreibung wird sowohl im Dialogfeld "Sammlungsmanager" als auch auf der Seite "Sammlung für dieses Profil auswählen" des Assistenten angezeigt, damit Sie die Sammlung leichter identifizieren können.
- **Regeln:** Angabe des Profilinhalts, der durch diese Sammlung migriert werden soll. Sie können die Strukturansicht durch Klicken auf die Felder mit dem Plus- oder Minuszeichen erweitern bzw. reduzieren, um alle Anwendungs-, Desktopeinstellungs- und Dateiregeln betrachten zu können. Zur Definition einer Sammlung können Sie die in der Strukturansicht "Regeln" angezeigten Regeln beliebig kombinieren.

Verwandte Themen

- Profilinhalt
- Übersicht über die Profilmigration

Informationen zum Dialogfeld "Benutzerinitiiertes Paket"

In diesem Dialogfeld können Sie eine selbstextrahierende ausführbare Datei erstellen, die auf Clients als benutzerinitiierte Profilmigration ausgeführt wird (klicken Sie im Dialogfeld "Sammlungsmanager" auf **Benutzerinitiierte Pakete** und anschließend auf **Neu**).

Hinweis: Benutzerinitiierte Pakete können sowohl auf von LANDesk verwalteten Clients als auch auf Computern, die nicht von LANDesk-Agenten verwaltet werden, ausgeführt werden.

- **Paketname:** Bezeichnung des benutzerinitiierten Pakets durch einen eindeutigen Namen. Wenn Sie den Namen eines vorhandenen Profilmigrationspakets eingeben, werden Sie gefragt, ob dieses überschrieben werden soll. Verwenden Sie einen Namen, der etwas über den Zweck und den Inhalt des benutzerinitiierten Pakets aussagt.

  Hinweis: Geben Sie hier keine Dateinamenerweiterung an; die Erweiterung .EXE wird automatisch an den eingegebenen Namen angehängt.

- **Regelsammlung:** Liste aller verfügbaren Regelsammlung. Die Sammlung, die Sie auswählen, bestimmt den Inhalt der benutzerinitiierten Profilmigration. Sie können nur eine Sammlung pro Migrationspaket auswählen.

Hinweis: Das benutzerinitiierte Migrationspaket (*.EXE) wird standardmäßig in folgendem Verzeichnis auf dem Core Server gespeichert: c:\Programme\LANDesk\ManagementSuite\LDLogon\PMScripts\Executables

---

Verwandte Themen

- Erstellen von benutzerinitiierten Profilmigrationspaketen
- Ausführen von benutzerinitiierten Profilmigrationspaketen
- Erstellen von Sammlungen
- Übersicht über die Profilmigration
- Profilinhalt

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Geben Sie Berechtigungsnachweise für die Profilspeicherung ein"

Auf dieser Seite geben Sie an, wo die Profildaten gespeichert und die Berechtigungsnachweise für die Authentifizierung zur Verfügung gestellt werden sollen.

- **UNC-Pfad zum Verzeichnis für die Profilspeicherung:** Angabe des UNC-Pfads für den Speicherort der Profildaten. Sie können den Computernamen einfach im UNC-Format angeben und dann die restliche Pfadangabe ergänzen, indem Sie auf die Schaltfläche "Durchsuchen" klicken.
- **Benutzername:** Angabe eines Benutzers, der für den angegebenen UNC-Pfad über gültige Berechtigungsnachweise für die Authentifizierung verfügt.
- **Kennwort:** Kennwort des Benutzers.
- **Domäne:** Domäne des Benutzers.
- **Authentifizierung mit diesen Berechtigungsnachweisen erzwingen:** Erzwingen einer Authentifizierung (Abmelden und Anmelden) unter Verwendung der oben angegebenen Berechtigungsnachweise bei Clients, die für eine Profilmigration eingeplant sind, WENN die Berechtigungsnachweise des gegenwärtig angemeldeten Benutzers nicht ausreichen. Mit dieser Option kann in einem solchen Fehlerfall sichergestellt werden, dass der Client über ausreichende Berechtigungen zum Lesen und Speichern von Daten auf der Netzwerkfreigabe verfügt, unter der die Profildaten gespeichert werden.
- **Standardkennwort für lokale(s) Benutzerkonto/en:** (Nur verfügbar bei einem Profilwiederherstellungsskript) Angabe eines Kennworts, das als gemeinsames Standardkennwort für alle *neu* migrierten lokalen Benutzerkonten dient, die auf dem Ziel-Client angelegt werden. Falls ein Benutzerkonto bereits vorhanden ist, werden die Einstellungen migriert, aber das aktuelle Kennwort wird beibehalten und muss bei der Anmeldung verwendet werden.

  Hinweis: Falls Sie dieses Textfeld leer lassen, wird für das Kennwort automatisch die Standardeinstellung übernommen: Kennwort

- **Fertigstellen:** Speichern des Skripts für die Profilmigration und Beenden des Assistenten.
- **Abbrechen:** Beenden des Assistenten, ohne das Skript zu speichern.

Verwandte Themen

- Übersicht über die Profilmigration

Informationen zum Betriebssystem-Verteilung/Migrationstasks-Assistenten: Seite "Geben Sie die DOS-Befehle für die Ausführung auf dem Client ein"

Auf dieser Seite können Sie ein Skript erstellen, das DOS-Befehle (einschließlich Namen von Anwendungsprogrammdateien) auf Ziel-Clients ausführt. Die einzelnen Befehle werden nacheinander an die Clients geschickt.

- **Textfeld "DOS-Befehl":** Diesem Textfeld können DOS-Befehle hinzugefügt werden, wobei Sie diese wie an der DOS-Eingabeaufforderung jeweils in einer eigenen Zeile eingeben müssen. Sie können beliebig viele Befehle eingeben.
- **Diesen Auftrag abbrechen, wenn ein Befehl fehlschlägt:** Bewirkt, dass der Abbildverarbeitungsauftrag abgebrochen wird, falls einer der auf dieser Seite eingegebenen DOS-Befehle fehlschlägt. Anwendungen (die von der DOS-Befehlszeile gestartet wurden), die im Fehlerfall einen DOS-Fehlerebenencode erzeugen, können ebenfalls den Abbruch des Abbildverarbeitungsauftrags bedingen. Führt der Fehlschlag eines Befehls oder einer Anwendung nicht zur Erzeugung eines Fehlerebenencodes, dann wird der Abbildverarbeitungsauftrag weiter ausgeführt.
- **Fertigstellen:** Speichern des DOS-Befehlsskripts und Beenden des Assistenten.
- **Abbrechen:** Beenden des Assistenten, ohne das Skript zu speichern.

Verwandte Themen

- Erstellen von Abbildverarbeitungsskripts mit dem Betriebssystem-Verteilung/Migrationstasks-Assistenten
- Übersicht über die Betriebssystem-Verteilung
- Übersicht über die Profilmigration

Anhang C: Zusätzliche Informationen zur Softwareverteilung

In diesem Kapitel wird beschrieben, wie Sie Enhanced Software Distribution (ESWD) von LANDesk Management Suite verwenden, um Software und Dateien über das Netzwerk an Clients zu verteilen.

In diesem Kapitel erfahren Sie mehr über:

- Skriptleitfaden für .CFG-Dateien
- Fehlerkorrektur für .CFG-Dateien und ihre Pakete
- Skriptleitfaden für Verteilungsskripts (.INI-Dateien)
- Bedeutung der Enhanced Software Distribution-Fehlercodes
- Dateien, die in Enhanced Software Distribution verwendet werden

Skriptleitfaden für .CFG-Dateien

In diesem Kapitel wird beschrieben, wie Sie Skripts und Skriptbefehle beim Erstellen eines Softwareverteilungspakets verwenden. Am Ende dieses Abschnitts finden Sie ein Beispielskript mit Anmerkungen zu den wichtigen Teilen des Skripts.

Detaillierte Anweisungen über das Erstellen und Ändern von .CFG-Dateien finden Sie in der Onlinehilfe von Package Builder. Klicken Sie auf **Start | Programme | LANDesk Management | LANDesk Enhanced Package Builder**. Klicken Sie auf **Hilfe | Index** und wählen Sie die folgenden Themen der Onlinehilfe aus:

- Erste Schritte mit Package Builder
- Erstellen einer einfachen Installation
- Package Builder-Befehle
- Wie erstellt Package Builder eine Installation?
- Verwenden von Variablen in Befehlen und Zuweisen von Werten

Skript-Grundlagen

Der Package Builder-Assistent führt Sie durch den Erstellungsvorgang für ein Softwareverteilungspaket. Der Assistent speichert die für die Ausführung der Installation auf anderen Computern erforderlichen Befehle. Er schreibt diese Befehle in eine ASCII-Datei mit einer .CFG-Erweiterung. Sie können diese Skriptdatei nach dem Erstellen in Package Builder öffnen; Sie können aber auch eine Skriptdatei neu erstellen und diese in das Paket integrieren.

Die Onlinehilfe von Package Builder enthält Syntaxinformationen für alle Skriptbefehle. Um auf die Hilfe wegen eines bestimmten Befehls zuzugreifen, markieren Sie den Befehl auf der linken Seite und drücken die Taste **F1**.

Um auf eine bestimmte Skriptdatei zuzugreifen, starten Sie Package Builder und klicken auf **Datei | Öffnen**. Durchsuchen Sie das Configs-Verzeichnis im Arbeitsverzeichnis von Package Builder und wählen Sie eine Datei aus.

Nachdem ein Skript geändert wurde, klicken Sie auf **Erstellen | Erstellen**, um das Skript in ein Paket zu integrieren.

Skriptbefehle

Jedes Skript umfasst zwei Abschnitte. Bestimmte Befehle am Beginn des Skripts definieren die Parameter und die restlichen Befehle beschreiben die Installation der Anwendung, die im Softwareverteilungspaket enthalten ist.

Alle in einem Skript enthaltenen Befehle können in eine dieser Funktionskategorien zusammengefasst werden:

- Basisinstallation
- Erscheinungsbild
- Meldungen & Eingaben
- Systemänderungen
- If-Bedingungen
- Standardwerte & Aufrufe

Diese Kategorien enthalten verwandte Befehle, die den Installationsvorgang für jedes Paket beschreiben. Einige Befehle beschreiben die für die Installation erforderlichen Parameter und müssen am Beginn der Skriptdatei stehen. Einzelheiten über jeden Befehl finden Sie in der Onlinehilfe zu Package Builder.

Bearbeiten von Paketen mit Package Builder

Die Benutzeroberfläche von Package Builder ist in drei Bereiche aufgeteilt:

- Auf der linken Seite sind die Funktionskategorien aufgeführt. Erweitern Sie jede Funktionskategorie, um die einzelnen Befehle innerhalb der Kategorien anzuzeigen.
- Die rechte Seite ist in zwei Bereiche aufgeteilt: Der obere Teil zeigt das Skript selbst an. Der untere Teil ist eine GUI-Vorlage, die Eingabefelder für die Parameter des markierten Befehls enthält.

Um die Einzelheiten eines Befehls im Skript anzuzeigen, markieren Sie den Befehl und zeigen die Parametereinzelheiten im unteren Teil des Bereichs an.

Um einen neuen Befehl zum Skript hinzuzufügen, wählen Sie die Stelle im Skript, an der der Befehl stehen soll. Markieren Sie dann den Befehl auf der linken Seite. Vervollständigen Sie nun die Syntaxvorlage im unteren Teil des Bereichs. Wenn Sie die Befehlsparameter ausgewählt haben, klicken Sie auf **Hinzufügen**, um den neuen Befehl einzufügen.

Verarbeiten von benutzerdefinierten Skripts

Benutzerdefinierte Skripts werden in drei Abschnitten verarbeitet:

- **Premachine**—Der Abschnitt "Premachine" des benutzerdefinierten Skripts wird zuerst nur einmal am Beginn des Task verarbeitet. Verwenden Sie diesen Abschnitt für Tasks, die keinen gezielten Client haben, und/oder für Targeted Multicast. Verwenden Sie im Premachine-Abschnitt des Skripts nur lokale Befehle, LOCxxx.
- **Rechner**—Die Befehle in diesem Abschnitt des Skripts werden anschließend und nur ein Mal pro Zielclient ausgeführt. Diese Befehle können entweder Fern- oder lokale Ausführungsbefehle verwenden und werden in erster Linie für die Fernausführung von SDCLIENT.EXE verwendet. Bevor die Befehle in diesem Abschnitt des Skripts durchgeführt werden können, muss der ESWD-Agent auf den Zielclients installiert werden.
- **Postmachine**—Dieser Abschnitt wird zuletzt und ebenfalls nur ein Mal verarbeitet, nachdem alle Clients verarbeitet wurden. Die Softwareverteilung fügt keine Befehle zu diesem Abschnitt hinzu und unterstützt nur die lokalen Befehle LOCxxx. Die Befehle in diesem Abschnitt werden nicht verarbeitet, wenn sie Clients im Task nicht ausführen können. Das Skript InventoryScanner.ini, das mit Management Suite geliefert wird, enthält Einzelheiten über die Skriptbefehle

Befehlszeilenparameter

Die Softwareverteilung wird durch ein Verteilungsskript erleichtert. SDCLIENT.EXE verwaltet die Pakete mithilfe von Befehlszeilenparametern aus der Skriptdatei, die an die Anwendung weitergegeben werden.

SDCLIENT.EXE unterstützt die folgenden Befehlszeilenparameter:

```
sdclient.exe /p="<package path>" [/g=<pkg guid>] [/All] [/R] [/N] [/An]
[/Ac] [/Ab] [/fui] [/msi] [/exe] [/bw=xxx] [/E]
```

Parametername	Beschreibung
/p=<package path>	Paketpfad. Der Paketpfad muss unabhängig von Pakettyp festgelegt werden. Dieser Parameter legt den UNC- oder URL-Pfad zum Paket fest, der auf dem lokalen Client installiert werden soll.
/g=<pkg guid>	Paket-GUID. Für ESWD- oder AutoInstall-Pakete. Dieser Parameter liegt die GUID für das Paket fest. Die Paket-GUID wird verwendet, um den lokalen .CFG-Dateicache auf eine Kopie der .CFG-Datei des Pakets zu überprüfen.
/All	Deinstallationskennzeichnung. Diese Kennzeichnung zeigt an, dass das ESWD- oder MSI-Paket lieber deinstalliert als installiert werden sollte. Bei dieser Kennzeichnung muss die Groß/Kleinschreibung beachtet werden (/all funktioniert nicht).
/R	Kennzeichnung, dass stets ein Neustart vorgenommen wird. Diese Kennzeichnung zeigt an, dass der Client nach der Paketinstallation stets neu gestartet werden soll. Nicht alle MSI-Pakete beachten diese Richtlinie.
/N	Kennzeichnung, dass nie ein Neustart vorgenommen wird. Diese Kennzeichnung zeigt an, dass der Client nie nach der Paketinstallation neu gestartet werden soll.
/An	Kennzeichnung für die stille Installation. Diese Kennzeichnung zeigt an, dass es sich um eine stille Installation handeln soll. Das bedeutet, dass keine oder nur ein möglichst kleiner Teil der Benutzeroberfläche während der Installation angezeigt werden soll.
/Ac	Kennzeichnung zum Deaktivieren des Abbruchs. Durch diese Kennzeichnung kann der Benutzer die Installation nicht abbrechen.
/Ab	Kennzeichnung, dass kein Hintergrund angezeigt wird. Diese Kennzeichnung gilt nur für ESWD-Pakete. Während der Installation eines Pakets wird der blaue Hintergrund nicht angezeigt.
/fui	Kennzeichnung für eine vollständige Benutzeroberfläche. Diese Kennzeichnung zeigt an, dass für Legacy- und MSI-Pakete die vollständige Benutzeroberfläche verwendet werden soll.

/msi	Kennzeichnung für MSI-Paket. Diese Kennzeichnung zeigt an, dass der Paketpfad auf eine MSI-Paketdatei verweist.
/exe	Kennzeichnung für ausführbare Paketdatei. Diese Kennzeichnung zeigt an, dass der Paketpfad auf ein Legacypaket oder eine generische ausführbare Datei verweist.
/Ah	Kennzeichnung für Application Healing Diese Kennzeichnung zeigt an, dass das Skript mit der Option auf Application Healing installiert wird.
/bw=xxx	Bandbreitenvoraussetzungen. Legt eine Mindestvoraussetzung für die Bandbreite fest, damit das Paketskript ausgeführt werden kann.
/F	Kennzeichnung für eine generische Datei. Durch diese Kennzeichnung lädt SDCLIENT.EXE die Datei in das Verzeichnis LDCLIENT herunter.

Einfaches Beispielskript

Dieses Skript enthält einige der Befehle, die für die Installation von Package Builder auf einem Computer verwendet werden, der Pakete erstellt. Wichtige Abschnitte oder Befehle werden mit Hinweisen (REM) versehen.

```
REM Dies ist die Installation von Package Builder

REM Bildschirmgrafik-Umgebung festlegen

SCREENCOLOR: (0,0,255), (0,0,255)

ANIMATION: "W:\Software\Install\Intel\duck\DISK01.BMP",
"W:\Software\Install\Intel\duck\DISK02.BMP",
"W:\Software\Install\Intel\duck\DISK03.BMP",
"W:\Software\Install\Intel\duck\DISK04.BMP",
"W:\Software\Install\Intel\duck\DISK05.BMP",
"W:\Software\Install\Intel\duck\DISK06.BMP",
"W:\Software\Install\Intel\duck\DISK07.BMP",
"W:\Software\Install\Intel\duck\DISK08.BMP",
"W:\Software\Install\Intel\duck\DISK09.BMP",
"W:\Software\Install\Intel\duck\DISK10.BMP",
"W:\Software\Install\Intel\duck\DISK11.BMP",
"W:\Software\Install\Intel\duck\DISK12.BMP",
"W:\Software\Install\Intel\duck\DISK13.BMP"

SCREENGRAPHIC: "W:\software\INSTALL\Intel\OAKLAN~1.BMP", topleft

REM TITLE: "LANDesk Management Suite", fontsize=25, color=yellow

REM SUBTITLE: "Package Builder", fontsize=18, italic, color=yellow

REM Konfigurieren von Deinstallationsoptionen

UNINSTALL: yes, removegroup, packagename="Package Builder"

UninstallBeginPrompt: "Möchten Sie die Programme und Verzeichnisse von
LANDesk Management Suite Package Builder von Ihrem System entfernen?"

UninstallEndPrompt: "Die Programme und Verzeichnisse von LANDesk
Management Suite Package Builder wurden erfolgreich von Ihrem System
entfernt."
```

```
REM Prüfen Sie vor der Installation, ob genügend
Festplattenspeicherplatz vorhanden ist

IF DISKSPACE() < 4000K

BEGINFIRSTSCREEN caption="Nicht genügend Speicherplatz", für Package
Builder sind 4 MB Festplattenspeicherplatz erforderlich. Reorganisieren
Sie Ihre Festplatte, sodass genügend Arbeitsspeicher zur Verfügung
steht.

ENDFIRSTSCREEN

REM Diese Meldung wird nur angezeigt, wenn weniger als 4 MB
Speicherplatz vorhanden sind.

ENDIF

REM Legen Sie den Splash-Bildschirmtext fest

BEGINFIRSTSCREEN caption="LANDesk Management Suite Package Builder",

Dieses Installationsprogramm richtet LANDesk Management Package Builder
auf der Festplatte ein. Wenden Sie sich an den LANDesk-Software-Customer
Support, wenn Probleme bei der Einrichtung auf Ihrem Computer auftreten
sollten.

ENDFIRSTSCREEN

REM Legen Sie das Standardverzeichnis fest, aus dem Sie arbeiten
möchten. Beachten Sie, dass die Variable $ProgFilesDir$ aus einer
Windows-Systemumgebungsvariablen stammt. Der Befehl DEFAULTDIR muss vor
dem Einsatz von Dateibefehlen verwendet werden.

DEFAULTDIR: "$ProgFilesDir$\Intel\Package Builder", prompt="Geben Sie
Laufwerk und Verzeichnis an:", caption="Verzeichnisname", text="Die
Software wird auf Ihrem System in einem Verzeichnis installiert.
Akzeptieren Sie das vorgeschlagene Verzeichnis, oder benennen Sie ein
eigenes Verzeichnis bzw. geben Sie es ein. Sie müssen sowohl einen
Laufwerksbuchstaben als auch den Verzeichnisnamen angeben."

REM Fügen Sie Dateien hinzu, die für alle Versionen von Package Builder
gelten. In diesem Beispielskript ist nur eine enthalten.

FILE: "CTL3D.000", overwrite=yes,
From="W:\Software\Install\Intel\CTL3D.DLL"

REM Installieren von Registrierungseinträgen

BEGINREGISTRY

KEY: new, "HKEY_CLASSES_ROOT\CFG"

VALUE: reg_sz, replace, "Standard", "txtfile"

ENDREGISTRY

REM Einrichten von Windows-Menüelementen

WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\Builder.exe",
"Package Builder", replace, allusers

WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\Replicator.exe",
"Package Builder wizard", replace, allusers

WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\ENUBLDRI.hlp",
"Package Builder wizard help", replace, allusers

REM Letzten Bildschirm definieren und anzeigen

BEGINLASTSCREEN caption="LANDesk Management Suite Package Builder",

Die Installation von Management Suite Enhanced Package Builder ist nun
abgeschlossen.

ENDLASTSCREEN
```

Registrierungsbefehle

Befehle, die die Registrierung ändern, beginnen und enden mit den Befehlen BeginRegistry und EndRegistry. Zwischen diesen Befehlen stehen die Befehle, die den Registrierungsschlüssel und den Wert kennzeichnen. Der Package Builder-Assistent kennzeichnet zwei Schlüssel als gefährlich:

- \HARDWARE
- \SYSTEM\CURRENTCONTROLSET

Diese Schlüssel gelten als gefährlich, da sie in der Regel nur mit Computern kompatibel sind, auf denen Pakete erstellt werden. Wenn diese Schlüssel geändert werden, platziert der Package Builder-Assistent solche Befehle mit der Anweisung IF $DANGEROUS$ = "TRUE". Wenn die Änderungen mit dem Zielcomputer kompatibel sind und Sie deren Ausführung wünschen, müssen Sie eine $DANGEROUS$-Variable am Beginn des Skripts definieren und für ihren Wert TRUE festlegen.

Starten eines Pakets aus einem Paket

Sie können INST32.EXE in der Befehlszeile eines RunAtExit-Befehls in einem Paket festlegen, um ein anderes Paket zu starten. Die Synatx lautet:

```
RunAtExit "INST32.EXE PACKAGENAME.EXE"
```

Wenn sich das Paket auf dem Netzwerk befindet, ist dies effizienter als die Ausführung von "PACKAGENAME.EXE", da Sie über einen HTTP-Pfad einen Paketnamen festlegen können. Beispiele:

```
http://myservername/packages/PACKAGENAME.EXE
```

Beispielskript mit komplexeren Befehlen

Dieses nächste Skript ist in Abschnitte aufgeteilt, die jeweils eine kurze Erklärung enthalten. Alle Anwendungen, die durch einen RunAtStart- oder RunAtMiddle-Befehl ausgeführt werden, müssen vor der weiteren Verarbeitung des Skripts geschlossen werden.

Im ersten Abschnitt dieses Skripts können Sie einen Fenstertitel, einen Paketnamen, animierte oder statische Grafiken, Ton sowie Farbe und Schriftart bestimmen. Über den Befehl RunAtStart können Sie eine externe Anwendung am Beginn der Installation ausführen.

Über den Befehl BeginFirstScreen können Sie dann die Benutzer über die Installation informieren, indem eine Textnachricht angezeigt wird. Der Backup-Befehl zeigt schließlich an, dass alle zu ersetzenden Dateien gesichert werden und der OverWriteFile-Befehl gibt an, dass der Benutzer zur Bestätigung aufgefordert wird, bevor vorhandene Dateien überschrieben werden.

```
ANIMATION: "C:\WINDOWS\CIRCLES.BMP", "C:\WINDOWS\CARVED~1.BMP",
"C:\WINDOWS\BUBBLES.BMP", "C:\WINDOWS\BLUERI~1.BMP",
"C:\WINDOWS\BLACKT~1.BMP"

RUNATSTART: "c:\programe\zubehör\mspaint.exe"

TITLE: "Package Builder-Funktionsskript für Windows 98", bold

INTROSCREEN: "C:\WINDOWS\SETUP.bmp", waittime=5, full
```

```
INTROSOUND: "C:\WINDOWS\MEDIA\START.WAV"
SCREENCOLOR: magenta, yellow
SCREENGRAPHIC: "C:\WINDOWS\PINSTR~1.BMP", topleft
FONTNAME: "Tahoma"
BEGINFIRSTSCREEN title="Erster Bildschirm", caption="Bildschirm #1"
Dieser Text wird auf dem ersten Bildschirm angezeigt.
ENDFIRSTSCREEN
BACKUP: JA
OVERWRITEFILE: ask
```

Die folgenden Beispiele zeigen verschiedene Eingabeaufforderungsoptionen. Der Text für jede Eingabeaufforderung kann geändert werden.

```
CancelPrompt: "Abbrechen?"
CopyFilePrompt: "UPLOAD WIRD DURCHGEFÜHRT"
OkPrompt: "FERTIG"
QuitPrompt: "Möchten Sie wirklich abbrechen?"
CopyTitlePrompt: "Wird kopiert..."
NextPrompt: "Weiter"
BackPrompt: "Zurück"
NoPrompt: "Nein"
YesPrompt: "Ja"
```

Dieser Abschnitt führt eine externe Anwendung aus und wartet darauf, dass diese Anwendung zum Fortfahren geschlossen wird. Wenn das Skript fortfährt, wird der Benutzer zur Eingabe aufgefordert. Basierend auf der gewählten Option fährt die Anwendung fort und kopiert eine Datei auf das lokale Laufwerk oder sie wird geschlossen.

```
RUNATMIDDLE: "c:\windows\calc.exe"
ASK1: Yesno, caption="Beispielfrage.", text="Dies ist ein Beispiel für
die Verwendung von Ja / Nein-Schaltflächen. Wählen Sie 'Ja', um
fortzufahren oder 'Nein', um zu schließen."
IF $ASK1$= "Ja"
WINGROUP: "Neue Programmgruppe", prompt="Gruppe wählen",
caption="Auswahl der Programmgruppe", text="Wählen Sie eine
Programmgruppe aus."
ELSE
IF $ASK1$= "Nein"
EXITMESSAGE
Schade, dass Sie bereits schließen!
EXIT
ELSE
ENDIF
ENDIF
PROGRESSBAR: 302K
COPY: "C:\windows\setup.bmp", "C:\windows\temp\p1.bmp"
```

```
RENAME: "C:\windows\temp\p1.bmp", "C:\windows\temp\renamed p1.bmp"
```

Dieser Abschnitt startet eine Anwendung als letzten Befehl, bevor das Skript abgeschlossen ist. Der RunAtExit-Befehl muss nicht die letzte Zeile des Skripts darstellen.

Dieser Abschnitt erstellt außerdem eine Verknüpfung auf dem Desktop sowie ein Deinstallationspaket.

```
RUNATEXIT: "C:\WINDOWS\CDPLAYER.EXE"

BEGINLASTSCREEN title="Letzter Bildschirm", caption="Der letzte
Bildschirm"

Dies sollte der letzte angezeigte Bildschirm sein.

ENDLASTSCREEN

SHORTCUT: "c:\windows\notepad.exe", "NOTEPAD", dir="c:\windows\desktop\"

UNINSTALL: yes, makeicon, removegroup, packagename="Package Builder-
Funktionalität"
```

HTTP- und UNC-Pfade

Dies sind Beispiele von .INI-Dateien für die Softwareverteilung, die die Unterschiede zwischen Skriptdateien für HTTP- und UNC-Pfad darstellen.

HTTP-Pfadskriptdatei:

```
; Diese Datei wurde von Desktop Manager erstellt

[MACHINES]

REMEXEC0=C:\ldclient/sdclient.exe -p=http://<web server>/packages/test
package.exe -g={6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-
9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

UNC-Pfadskriptdatei:

```
; Diese Datei wurde von Desktop Manager erstellt

[MACHINES]

REMEXEC0=C:\ldclient\sdclient.exe -p=\\sample_core\onefile\test
package.exe -g={6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-
9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

Beachten Sie, dass beide .INI-Dateien ähnliche Elemente enthalten. Im Abschnitt MACHINES bezeichnet die Option -P den Pfad, von dem der Client das Softwarepaket herunterlädt. Im HTTP-Beispiel ist der Pfad http://<web server>/packages/test package.exe.

Die nächste Option ist die Option -G, die GUID, eine eindeutige numerische Kennung für jedes Paket. Diese numerische Kennung wird durch Package Builder generiert und unterstützt die Vermeidung von Verwechslungen zwischen Paketen mit ähnlichen Namen bei der Installation.

Fehlerkorrektur für .CFG-Dateien und ihre Pakete

Der erste Schritt bei der Fehlerbehebung in Skripts besteht in der Festlegung, was funktioniert und was nicht. Hier finden Sie einige Tipps zur Fehlerkorrektur, die Ihnen beim Beheben von Skriptfehlern nützlich sein können:

- Erstellen Sie ein neues Skript, das nur aus dem Teil des Skripts besteht, das für den Fehler verantwortlich ist. Prüfen Sie die Funktion des Skripts und nehmen Sie die gewünschten Änderung mithilfe der Online-Befehlshilfe vor.
- Vergleichen Sie das neue Skript mit einem vorhandenen Skript, um Syntaxfehler festzustellen.

Verwenden Sie die folgenden Richtlinien, wenn Sie Pakete auf dem Computer erstellen, der für die Paketerstellung zuständig ist. Diese Tipps helfen Ihnen dabei, überflüssige Fehler zu vermeiden.

Verwenden von Befehlen

Geben Sie keine Variablen an den Befehl "DLL Load" in Package Builder weiter

Wenn Sie ein Paket erstellen, das von der Weitergabe einer Variablen an den Befehl "DLL Load" abhängt, muss die Variable zum richtigen Zeitpunkt ankommen. Wenn die .DLL die erwartete Variable nicht erhält, kann das Paket die Installation nicht richtig abschließen. Sie vermeiden dieses Problem, indem Sie keine Variablen an den Befehl "DLL Load" weitergeben; die anderen DLL-Parameter funktionieren korrekt.

Verwenden der Package Builder-Befehle "RunAtMiddle", "RunAtStart" und "RunAtExit"

Die Package Builder-Befehle "RunAtMiddle", "RunAtStart" und "RunAtExit" erfordern den vollständigen Pfad, damit die ausführbare Datei korrekt ausgeführt wird. Außerdem muss der Befehl "RunAtMiddle" im Skript nach der Funktion DEFAULTDIR stehen, damit er richtig funktioniert. Die Befehle "RunAtStart" und "RunAtExit" können an beliebiger Stelle im Skript stehen; sie werden stets richtig ausgeführt.

Neustart während der Paketerstellung

Wenn Sie den Package Builder-Assistenten verwenden, um ein Paket zu erstellen, werden Sie möglicherweise zum Neustart des Computers aufgefordert, auf dem das Paket erstellt wird. In vielen Fällen führt ein Neustart vor dem Abschließen der Paketerstellung dazu, dass das Paket nicht korrekt auf dem Client erstellt wird. Die Anwendung wird dann für den Computer konfiguriert, auf dem das Paket erstellt wird und nicht für den Zielclient. In manchen Fällen ist jedoch ein Neustart erforderlich, da das Installationsprogramm auf die Installations-CD nach dem Neustart zugreift.

Sie müssen das resultierende Paket prüfen, um festzustellen, ob Sie den Installationsvorgang stoppen und das Paket vor dem Neustart erstellen können oder ob Sie während der Softwareinstallation einen Neustart des Computers durchführen müssen und dann mit der Erstellung des Pakets fortfahren.

Erstellen und Benennen von Softwareverteilungspaketen

Paketnamen können nach ihrer Erstellung nicht geändert werden

Sie können einen Paketnamen nicht ändern, nachdem Sie die Paketerstellung abgeschlossen haben. Wenn Sie versuchen, den Dateinamen direkt zu ändern, können die Benutzer auf dieses Paket nicht richtig zugreifen.

Paketnamen dürfen keine Bindestriche oder Punkte enthalten

Wenn Sie Bindestriche oder Punkte in Paketnamen verwenden, schneidet der Paketerstellungsvorgang den Namen ab. Sie können immer noch auf das Paket in einem Skript zugreifen und Benutzer können es installieren, aber der abgeschnittene Namen könnte zu Verwirrungen führen. Verwenden Sie in Paketnamen weder Bindestriche noch Punkte. Sie können stattdessen das Unterstrichzeichen (_) verwenden.

Wir empfehlen Ihnen, bei jeder Neuerstellung eines Pakets in neues Arbeitsverzeichnis zu erstellen. Um dieses Verzeichnis zu erstellen, starten Sie den Package Builder-Assistenten und klicken auf **Scanoptionen.** Geben Sie im Feld "Temporäres Arbeitsverzeichnis" entweder den vollständigen Pfad zu einem Verzeichnis ein oder suchen sie nach ihm. Package Builder fordert Sie zur Bestätigung auf, ob Sie der Erstellung eines nicht bereits vorhandenen Verzeichnisses zustimmen.

Speichern Sie Softwareverteilungspakete nur im Verteilungspfad

Im Webserverpfad oder im UNC-Ordner sollten Sie nur Pakete speichern, die Sie für die Softwareverteilung einrichten. Wenn Sie andere Typen von ausführbaren Dateien in diesem Ordner speichern, könnte dies zu Verwechslungen mit Paketen führen, wenn Sie Verteilungspaketskripts erstellen. Wenn Sie ein Verteilungsskript für eine ausführbare Datei erstellen, die kein Paket ist, schlägt die Verteilung fehl. Speichern Sie Softwareverteilungspakete nur im Verteilungspfad.

Detaillierte Anweisungen über das Erstellen und Ändern von Paketen finden Sie in der Onlinehilfe von Package Builder unter "Arbeiten mit Package Builder".

Dateisammlungen können nicht mehr als 296 Dateien enthalten

Wenn Sie ein Dateisammelpaket erstellen, können Sie 296 separate Dateien oder Ordner hinzufügen. Wenn Sie versuchen, mehr als 296 Elemente hinzuzufügen, wird die Dateisammlung angehalten. Dateien, die in einem eingeschlossenen Ordner enthalten sind, zählen als ein Element, nicht als separate Dateien.

Skriptleitfaden für Verteilungsskripts (.INI-Dateien)

Sie müssen nicht das Fenster "Verteilungspaketskript erstellen" verwenden, um die Verteilungsskriptdatei zu erstellen. Eine Verteilungsdatei ist eine .INI-Datei, die die Einstellungen enthält, die der Client für die Paketinstallation verwenden soll. Sie können Ihre eigenen Verteilungsdateien in einem Texteditor wie Notepad auch selbst erstellen.

Eine .INI-Datei für die Softwareverteilung besteht aus den folgenden Komponenten:

```
[MACHINES]
```

```
REMEXEC0=C:\ldclient\sdclient.exe
/p="http://computer_name/95Packages/Acro32_95.exe"
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-
66E3BC2DF01A0D4B2F88670DE4}
/Ac
/N
```

REMEXEC0 Befehlsparameter
Die Parameter für den Befehl REMEXEC0 wurden in separate Zeilen eingefügt, um die Komponenten deutlicher hervorzuheben. In einer .INI-Datei muss sich der Befehl in einer Zeile befinden.

REMEXEC0 ist der Fernausführungsbefehl. Wenn Sie mehr als einen REMEXEC0-Befehl in einer einzelnen Skriptdatei verwenden möchten, erhöhen Sie den Befehl bei jeder Verwendung. Wenn Sie z.B. drei REMEXEC-Aufrufe in einer .INI-Datei verwendet haben, sollten sie REMEXEC0, REMEXEC1 und REMEXEC2 heißen. Die Befehle müssen nicht inkrementiert werden, wenn sie sich in separaten Dateien befinden.

Der Parameter c:\Ldclient\SDCLIENT.EXE ist der richtige Pfad zum ESWD-Agenten.

Der Parameter /p gibt den Pfad an, unter dem der Client das Paket herunterladen kann.Beispiel:

```
/p="http://computer_name/95Packages/Acro32_95.exe"
```

Der Parameter /g verweist auf eine GUID-Kennzeichnungsnummer für das Paket.Beispiel:

```
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-
66E3BC2DF01A0D4B2F88670DE4}
```

Wenn Sie diesen Parameter verwenden, lädt der Client nur das Paket mit genau dieser ID-Nummer herunter. Verwenden Sie das Fenster "Verteilungspaketskript erstellen", um diese ID-Nummer zu generieren, da sie in das Softwarepaket eingebettet ist.

Der Parameter /Ac verbirgt die Installation gegenüber den Benutzern. Sie können die Installation nur abbrechen, wenn Sie zu einer Aktion aufgefordert werden. Der Parameter /Ab verbirgt den Hintergrund. Der Parameter /An verbirgt die gesamte Benutzeroberfläche und verhindert jegliche Interaktion (Eingabeaufforderungen) für die Benutzer.

Der Parameter /Ah+ repariert ein zuvor installiertes Paket, ohne den Benutzer zu einer Eingabe aufzufordern.Der Parameter /A- installiert ein zuvor installiertes Paket neu, ohne den Benutzer zu einer Eingabe aufzufordern.

Der Parameter /N erzwingt keinen Neustart des Computers, auf dem das Paket installiert wurde. Der Parameter /R erzwingt einen Neustart des Computers, auf dem das Paket installiert wurde. Wenn Sie weder den Parameter /N noch den Parameter /R verwenden, wird der Computer nur dann neu gestartet, wenn verwendete Dateien aktualisiert wurden oder ein Neustart erforderlich ist, um die Installation abzuschließen.

Ein optionaler Parameter /D öffnet ein Fenster für die Fehlerkorrektur, um operative Parameter für SDCLIENT.EXE anzuzeigen. Das Fehlerkorrekturfenster zeigt den Paketpfad und den Namen, die GUID, etwaige Fehler- oder Meldungscodes und den Abschlusscode an, der zum Fenster "Geplante Tasks" zurückgegeben wurde.

Wenn das Softwareverteilungsskript die vorhandene Anwendung deinstallieren soll, können zwei Parameter für die Deinstallationsoption verwendet werden:

- Der Parameter /Au deinstalliert die letzte Instanz eines Pakets und führt einen Rollback einer Installationsinstanz durch.
- Der Parameter /All deinstalliert alle Instanzen eines Pakets und entfernt das gesamte Paket.

Wenn Sie sich an diese Richtlinien halten, können Sie eigene Softwareverteilungsskripts erstellen und ihre Versendung an Clients planen.Diese Skripts werden im Ordner DTM\Scripts auf dem Core Server gespeichert.

Bedeutung der Enhanced Software Distribution-Fehlercodes

Auf der Konsole wird auf der rechten Seite des Fensters "Geplante Tasks" der Status der Verteilung angezeigt. Wenn der Vorgang abgeschlossen ist, wird auf der Seite entweder eine Erfolgsmeldung oder eine Erklärung für das Fehlschlagen angezeigt. Zusätzlich hat jeder Zielclient Protokolldateien, die Daten über die Verteilung enthalten. Status und Fehler werden in folgenden Dateien aufgezeichnet:

- Wenn der Fehler beim Versuch des Zugriffs auf das Paket aufgetreten ist, wird er in der Datei AICLIENT.LOG protokolliert.
- Wenn der Fehler bei der Verarbeitung des Pakets (z.B. beim Kopieren von Dateien) aufgetreten ist, wird er in der Datei INST32.LOG protokolliert.
- Die Datei SDCLIENT.LOG enthält eine allgemeine Zusammenfassung über jede Installationsanforderung, die vom Core Server empfangen wird.

Diese Protokolldateien werden auf dem jeweiligen Client gespeichert.Die folgende Tabelle enthält die Fehlercodes, die in diesen Dateien enthalten sein können.

Fehlercode	Definition
101	Der Benutzer hat die Installation abgebrochen.
102	Der Dateizugriff wurde verweigert.
103	Das verwendete Kennwort ist ungültig.
104	Netzwerk nicht gefunden oder falscher Pfad angegeben.
105	Es ist ein Fehler beim Herunterladen aufgetreten.
106	Es konnte kein Sockel erstellt werden.
107	Es konnte keine HTTP-Sitzung geöffnet werden.
108	Es ist ein Fehler beim Herunterladen von CFG aufgetreten.
109	Es ist ein Fehler beim Speichern von CFG aufgetreten.
110	Es ist kein CFG-Ordner zum Speichern vorhanden.
111	Es ist ein Fehler beim Dateizugriff aufgetreten.

112	Es ist ein Fehler beim Abruf von CFG aufgetreten.
113	Es konnte keine CFG-Sicherungskopie erstellt werden.
114	Ein Spawn-Fehler ist aufgetreten, weil gerade ein anderes Paket installiert wird.
117	Das Sicherungsverzeichnis kann nicht erstellt werden.
180	Netzwerkfehler. Initialisierung nicht möglich.
188	Timeout während des Herunterladens über HTTP.
189	HTTP-Verbindung abgebrochen.
191	Host nicht gefunden.
197	HTTP-Datei nicht gefunden.
201	Die UNC-Datei kann nicht gefunden werden.
202	Die Datei konnte auf der Installationsdiskette nicht gefunden werden.
203	In festgelegtem Pfad konnte keine Datei erstellt werden.
204	Nicht genügend Speicherplatz auf dem Ziellaufwerk für die Installation.
205	Es wurde ein ungültiges Laufwerk angegeben oder das für diese Installation erforderliche Laufwerk war nicht verfügbar.
206	Die Datei hat einen langen Dateinamen und kann nicht durch das 16-Bit-Installationsprogramm installiert werden. Sie können weiterhin mit der Installation von anderen Dateien fortfahren.
207	Die angegebene Datei ist keine ausführbare Datei.
208	Innerhalb desselben Quellpfads sind mehrere Deinstallationseinträge in der Registrierung vorhanden.
209	Die ausführbare Datei für die Deinstallation konnte nicht gefunden werden.
210	Es wurde eine ungültige komprimierte Datei gefunden oder es liegt ein HTTP-Fehler vor.
211	Vor Verwendung dieser API muss ein erfolgreicher AFXSOCKETINIT-Befehl

	vorliegen.
212	Das Netzwerksubsystem ist fehlgeschlagen.
213	Keine weiteren Dateibeschreibungen verfügbar.
214	Der Sockel kann nicht erstellt werden. Es war kein Puffer vorhanden.
215	Die angegebene Adresse wurde bereits verwendet.
216	Der Verbindungsversuch wurde abgelehnt.
217	Die angegebene Hostadresse war ungültig.
218	Das Netzwerk kann zu diesem Zeitpunkt nicht vom Host erreicht werden.
219	Beim Verbindungsversuch ist ein Timeout aufgetreten, ohne dass eine Verbindung eingerichtet werden konnte.
220	Der virtuelle Schaltkreis wurde wegen eines Timeouts oder anderen Fehlers unterbrochen.
221	Der virtuelle Schaltkreis wurde an der Fern-Site zurückgesetzt.
222	Es ist ein nicht festgelegter HTTP-Fehler aufgetreten.
223	Ein HTTP-Fehler ist aufgetreten; die Datei war nicht geöffnet zum Lesen.
224	Ein HTTP-Fehler ist aufgetreten; es wurde keine Einstellung für die Inhaltslänge angegeben.
225	Ein HTTP-Fehler ist aufgetreten; es ist nicht genügend Speicherplatz vorhanden.
226	Ein Speicherzuweisungsfehler ist aufgetreten.
227	Datei kann nicht gelesen werden.
228	Unzureichender Speicherplatz.
229	Die .CFG-Datei enthält einen Fehler in Zeile XX.
240	Der angegebene temporäre Pfad ist ungültig. Zugriff oder Erstellung nicht möglich. Auf dem Zielcomputer liegt ein Konfigurationsproblem vor.

301	Diese Anwendung wurde nie auf diesem Computer installiert; Deinstallation nicht möglich.

Dateien, die in Enhanced Software Distribution verwendet werden

Dies ist eine Liste der Dateien, die in ESWD verwendet werden. Sie enthält außerdem Beschreibungen, wie diese zusammen funktionieren. Sie können diese Informationen verwenden, um anzupassen, wie Pakete in Ihrem Unternehmen verteilt werden.

Diese Dateien werden auf dem Core Server installiert:

- ManagementSuite\CUSTJOB.EXE
- ManagementSuite\SDMAKINI.DLL
- ManagementSuite\LANDesk.ManagementSuite.WinConsole.dll
- ManagementSuite\INSTALL\EN_PKG_BLDR\SETUP.EXE
- ManagementSuite\LDLOGON\SDCLNSTL.EXE

Diese Dateien werden auf dem Client installiert:

- C:\LDCLIENT\SDCLIENT.EXE
- C:\LDCLIENT\AICLIENT.DLL
- C:\LDCLIENT\SDMCACHE (dies ist ein leerer Ordner)
- C:\LDCLIENT.LOG (this file is created by the SDCLIENT.EXE file)
- INST32.EXE
- EUNINST32.DLL (oder andere lokalspezifische Ressourcendatei)
- $WINDIR$\aiclient.log
- $WINDIR$\aiclient.log

Dateibeschreibungen

SETUP.EXE: Diese eigenständige, binäre Installationsdatei wird verwendet, um Computer einzurichten, auf denen Pakete erstellt werden und um Package Builder, Package Builder-Assistenten-Tools und begleitende Dateien der Onlinehilfe auf dem Computer zu installieren. Aus jeder Anwendung, die Sie mit Package Builder zusammenpacken, wird eine selbstextrahierende .EXE-Datei.

Wenn Sie die Webkonsole verwenden, müssen Sie die .EXE in das Paketverzeichnis auf dem Webserver kopieren, damit Benutzer darauf zugreifen können.

SETUP.EXE installiert die folgenden Dateitypen auf dem Computer, auf dem Pakete erstellt werden, im Verzeichnis Programmdateien\Intel\Package Builder:

- BUILDER.EXE: Ausführende Datei von Enhanced Package Builder
- ENUBLDR.DLL: Ressourcendatei von Enhanced Package Builder
- REPLICATOR.EXE: Ausführende Datei des Package Builder-Assistenten
- ENUREPLC.DLL: Ressourcendatei des Package Builder-Assistenten
- BASIC.CFG: Ein einfaches Installationsskript für das Erstellen eines Softwareverteilungspakets
- TYPICAL.CFG: Ein komplexeres Installationsskript für das Erstellen eines Softwareverteilungspakets
- ENUBLDR.HLP: Hilfedatei für Package Builder
- ENUBLDRI.HLP: Hilfedatei für den Package Builder-Assistenten

CUSTJOB.EXE: Diese Datei wird direkt von Scheduler gestartet, wenn ein Auftrag beginnen soll.

SDC_INSTALL.INI: Das Auftragskript wird durch CUSTJOB.EXE verarbeitet. Es kopiert SDCINSTL.EXE auf einen Ferncomputer und führt sie dann auf diesem Computer über Common Base Agent (CBA) aus. Diese Datei befindet sich im Ordner DTM\Scripts.

SDCLNSTL.EXE: Diese Datei installiert die ESWD-Clientdateien SDCLIENT.EXE und AICLIENT.DLL auf Windows 95/98- und Windows NT/2000/2003/XP-Clients. Diese Datei befindet sich im Ordner DTM\LDLogon auf dem Core Server.

SDCLIENT.EXE: Diese Datei befindet sich letztendlich im Ordner C:\LDClient auf dem Client. Sie wird mit Befehlszeilenparametern aufgerufen, die den URL- oder UNC-Pfad des zu installierenden Verteilungspakets beinhalten. Dieser Aufruf ist in der Regel ein Ergebnis des Schedulers des Core Servers, der CUSTJOB.EXE aufruft.

AICLIENT.DLL: Diese Datei wird durch SDCLIENT.EXE aufgerufen; sie wird in denselben Ordner kopiert wie SDCLIENT.EXE.

INST32.EXE: Dies ist das eigentliche Installationsprogramm. Es ist in jedes selbstextrahierende Paket eingebettet. Es wird außerdem im Verzeichnis LDClient installiert und durch SDCLIENT.EXE immer dann gestartet, wenn eine Aufforderung zur Installation des Softwarepakets empfangen wird.

ENUINST32.DLL: Dies ist die lokalspezifische Ressourcendatei. Ihr Name hängt vom Gebiet ab.

AICLIENT.LOG: Dies ist ein rollierendes Protokoll. Sobald es 50 KB überschreitet, wird es durch die nächste Installation umbenannt in AICLIENT.LOG1. Wenn die neue AICLIENT.LOG-Datei die Grenze von 50 KB überschreitet, wird AICLIENT.LOG1 umbenannt in AICLIENT.LOG2. Sie wird erneut erhöht auf AICLIENT.LOG3. Sie wird gelöscht, wenn das nächste Mal die 50 KB-Grenze überschritten wird in der aktuellen AICLIENT.LOG-Datei.

INST32.LOG: Dies ist ein rollierendes Protokoll. Sobald es 50 KB überschreitet, wird es durch die nächste Installation umbenannt in INST32.LOG1. Wenn die neue INST32.LOG-Datei die Grenze von 50 KB überschreitet, wird INST32.LOG1 umbenannt in INST32.LOG2. Sie wird erneut erhöht auf INST32.LOG3. Sie wird gelöscht, wenn das nächste Mal die 50 KB-Grenze überschritten wird in der aktuellen INST32.LOG-Datei.

Informationen über den Paketbereitstellungsassistenten

Die folgenden Abschnitte beschreiben die Seiten und Optionen des Paketbereitstellungsassistenten.

Info über die Seite "Paket bereitstellen"

Wählen Sie auf dieser Seite das Paket aus, das Sie verteilen möchten.

- **Webpfad:** Klicken Sie auf "Webpfad", um Pakete anzuzeigen, die auf einem Webserver gespeichert sind. Sie müssen http:// in die URL-Angabe mit einschließen.
- **Dateifreigabepfad:** Klicken Sie auf "Dateifreigabepfad", um Pakete anzuzeigen, die in einer Nullsitzungsfreigabe auf einem Dateiserver gespeichert sind. Dieser Pfad muss den UNC-Pfadkonventionen \\servername\freigabename\ entsprechen.
- **Durchsuchen:** Klicken Sie auf **Durchsuchen**, um nach dem Pfad zu suchen. Wenn Sie auf **Webpfad** geklickt haben, wird ein kleines Fenster zum Durchsuchen angezeigt. Wenn Sie auf **Dateifreigabepfad** geklickt haben, wird ein Standarddialogfeld zum Durchsuchen angezeigt.

Info über die Seite "Anwendungsrichtlinie erstellen"

Auf dieser Seite geben Sie den Skripttyp an. Es stehen Ihnen verschiedene Optionen zur Verfügung, abhängig vom Paket, das Sie bereitstellen. **Installieren** und **Deinstallieren** sind nur verfügbar, wenn das Paket ein ESWD- oder ein MSI-Paket ist.

- **Skriptname:** Geben Sie einen beschreibenden Namen für das Skript ein, das Sie erstellen.
- **Installieren:** Legt fest, dass Sie ein Installationspaket verwenden möchten, um die Software zu installieren.
- **Deinstallieren:** Legt fest, dass Sie ein Installationspaket verwenden möchten, um die Software zu entfernen. Wenn diese Kennzeichnung festgelegt ist, entfernt das Skript alles, was mit dem Installationsskript installiert wurde.

Info über die Seite "Skript erstellen"

Auf dieser Seite geben Sie den Skripttyp an. Es stehen Ihnen verschiedene Optionen zur Verfügung, abhängig vom Paket, das Sie bereitstellen. **Installieren** und **Deinstallieren** sind nur verfügbar, wenn das Paket ein ESWD- oder ein MSI-Paket ist. Für Macintosh OS 10.2-Skripts steht nur das Feld "Skriptname" zur Verfügung.

- **Skriptname:** Geben Sie einen beschreibenden Namen für das Skript ein, das Sie erstellen.
- **Installieren:** Legt fest, dass Sie ein Installationspaket verwenden möchten, um die Software zu installieren.

- **Deinstallieren:** Legt fest, dass Sie ein Installationspaket verwenden möchten, um die Software zu entfernen. Wenn diese Kennzeichnung festgelegt ist, entfernt das Skript alles, was mit dem Installationsskript installiert wurde.
- **Verteilen Sie dieses Paket mit Multicast.** Aktiviert Targeted Multicast, sodass mehrere Computer dieselbe Verteilung gleichzeitig erhalten.
- **Nur Dateien auf dem Computer cachen, die Multicast verwenden:** Diese Option steht zur Verfügung, wenn "Multicast verwenden" aktiviert ist, um dieses Paket zu verteilen. Diese Option sendet nur die ausgewählte Datei bzw. das Paket per Multicast an das Multicast-Cacheverzeichnis des Zielcomputers (SDMCACHE). Dadurch können künftige Auftragsverteilungen möglicherweise schneller durchgeführt werden.

  Wenn Sie diese Option verwenden, um eine Datei oder ein Paket zu Clients zu senden, sucht das nächste Mal, wenn Sie einen Verteilungsauftrag starten, der diese Datei verwendet, jeder Client in seinem Verzeichnis SDMCACHE nach der ersten Datei, bevor ein Webserver oder UNC-Pfad geprüft wird. Auf jedem Client, bei dem die Datei lokal gespeichert ist, wird dann das Paket aus dem Verzeichnis SDMCACHE installiert, ohne dass zusätzliche Bandbreite für die Dateiübertragung verwendet wird. Wenn diese Option ausgewählt ist, deaktiviert sie die Installations- und Deinstallationsoptionen.

Info über die Seite "Multicast-Domänenoptionen"

Diese Seite wird nur angezeigt, wenn Sie "Multicast" als Verteilungstyp ausgewählt haben. Auf dieser Seite konfigurieren Sie Multicast-Optionen.

- **Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Auftrag durchzuführen. Bei dieser Option werden die Domänenerkennungsergebnisse für die erneute Verwendung nicht gespeichert.
- **Multicast-Domänenerkennung verwenden und Ergebnisse speichern:** Verwenden Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Auftrag durchzuführen und die Ergebnisse für eine künftige Verwendung zu speichern; somit sparen Sie Zeit bei folgenden Multicasts
- **Ergebnisse der letzten Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option immer dann, wenn Sie durch Targeted Multicast eine Domänenerkennung durchgeführt haben und speichern Sie die Ergebnisse.
- **Domänenvertreter muss Computer reaktivieren:** Verwenden Sie diese Option, wenn Sie Computer, die die "Wake On Lan*"-Technologie unterstützen, beim Empfang von Multicast reaktivieren möchten. Sie können das Dialogfeld "Multicast-Optionen" verwenden, um zu konfigurieren, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das "Wake on Lan"-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden.
- **Erweiterte Multicast-Optionen:** Verwenden Sie diese Option, um erweiterte Optionen festzulegen. Die Standardeinstellungen sind für die meisten Aufträge geeignet.

Infos über die Domänenerkennung

Die Domänenerkennung ist nur auf Netzwerken mit Subnetzen erforderlich, die gegenseitig ihren Multicast-Datenverkehr erkennen können. Wenn Ihre Subnetze den gegenseitigen Datenverkehr nicht erkennen können, sparen Sie Zeit, indem Sie **Ergebnisse der letzten Multicast-Domänenerkennung verwenden** auswählen; Targeted Multicast muss dann nicht vor jedem Auftrag eine Domänenerkennung durchführen.

Wenn Ihre Netzwerksubnetze den gegenseitigen Multicast-Datenverkehr nicht erkennen können, können Sie Targeted Multicas dabei unterstützen, schneller zu funktionieren, indem Sie die Domänen vorab identifizieren mithilfe des Skripts multicast_domain_discovery.ini, das sich im Verzeichnis DTM\Scripts befindet. Dieses Skript führt auf Zielcomputern keine Vorgänge durch. Führen Sie dieses Skript aus dem Fenster "Geplante Tasks" auf eine Zielliste aus, die das Netzwerk umfasst. Die Domänenerkennungsergebnisse werden dadurch für die künftige Verwendung gespeichert. Sie können dieses Skript regelmäßig vor großen Sätzen von Multicast-Verteilungen ausführen.

Wenn Sie **Cachedatei verwenden** unter **Management Suite-Dienste konfigurieren | Multicast** ausgewählt haben, durchläuft Targeted Multicast einen Suchvorgang, auch wenn Sie **Ergebnisse der letzten Multicast-Domänenerkennung verwenden** ausgewählt haben. Targeted Multicast muss dies durchführen, um herauszufinden, welche potenziellen Multicast-Domänenrepräsentanten die Datei in ihrem Cache gespeichert haben.

Infos über die Seiten "Multicast - Zusätzliche Dateien" und "Bereitzustellende Dateien auswählen"

Die Seite "Multicast - Zusätzliche Dateien" wird angezeigt, wenn Sie eine "Multicast Software Distribution" durchführen. Die Seite "Bereitzustellende Dateien auswählen" wird im Dateiübertragungsskript-Assistenten angezeigt. Die Seiten sind identisch, abgesehen von ihrem Titel. Verwenden Sie diese Seite, um zusätzliche Dateien auszuwählen. Sie können jeweils eine Datei auswählen.

- **Webpfad:** Klicken Sie, um auf einem Webserver gespeicherte Pakete anzuzeigen. Sie müssen http:// in die URL-Angabe mit einschließen.
- **Dateifreigabepfad:** Klicken Sie, um Pakete in einer Nullsitzungsfreigabe auf dem Dateiserver anzuzeigen. Dieser Pfad muss den UNC-Pfadkonventionen \\servername\freigabename\ entsprechen.
- **Durchsuchen:** Klicken Sie auf **Durchsuchen**, um nach dem Pfad zu suchen. Wenn Sie auf **Webpfad** geklickt haben, wird ein kleines Fenster zum Durchsuchen angezeigt. Wenn Sie auf **Dateifreigabepfad** geklickt haben, wird ein Standarddialogfeld zum Durchsuchen angezeigt. Wenn Sie im Browserfenster "Paketspeicherort auswählen" ein Webserververzeichnis durchsuchen möchten, müssen Sie die URL mit einem nachgestellten Schrägstrich (/) angeben, da das Browserfenster sonst einen Fehler anzeigt.
- **Hinzufügen:** Verwenden Sie **Hinzufügen**, um ein Programm direkt aus dem Pfadbearbeitungsfeld hinzuzufügen, nachdem Sie den vollständigen Pfad und den Dateinamen eingegeben haben.
- **Entfernen:** Wählen Sie eine Datei aus, die Sie hinzugefügt haben und klicken Sie auf **Entfernen**, um eine Datei aus der Liste zu entfernen.

Infos über die Seite "Download-Optionen"

Auf dieser Seite konfigurieren Sie die Bandbreitendrosselung und Paketverzögerungen.

- **Peerdownload (nur vom Cache oder Peer installieren):** Lässt das Herunterladen von Paketen nur dann zu, wenn sie sich im lokalen Cache oder auf einem Peer in der gleichen Multicast-Domäne befinden. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Paketinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sich das Paket im lokalen Cache oder im Cache eines Peer befindet. Eine Möglichkeit zur Nutzung dieser Option besteht darin, das Paket zuerst mit der Option **Nur Dateien auf dem Computer cachen, die Multicast verwenden**, die an früherer Stelle im Assistenten verfügbar ist, auf einen Client in jedem Subnetz zu kopieren.
- **Dynamische Bandbreitendrosselung:** Legt fest, dass der von einem Client erzeugte Netzwerkverkehr Vorrang vor dem durch die Verteilung bedingten Verkehr hat. Wenn Sie diese Option auswählen und die Angabe für **Minimal verfügbare Bandbreitenprozentsatz** auf 0 belassen, wird die Verteilung auf etwa ein Paket pro Sekunde gedrosselt, sobald der Client Netzwerkverkehr initiiert, und bleibt auf diesem Niveau, bis der Netzwerkverkehr endet.
  Diese Option erzwingt, dass die gesamte Datei in den Cache des Clients heruntergeladen wird. Damit wird gleichzeitig die Option für Checkpoint-Neustarts auf Byte-Ebene aktiviert, sodass Downloadvorgänge im Fall einer Unterbrechung an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden,. Wenn Sie ein ESWD- oder MSI-Paket erneut installieren oder reparieren, sollten Sie die Option **Dynamische Bandbreitendrosselung** nicht verwenden, weil bei diesen Pakettypen normalerweise nur die benötigten Dateien heruntergeladen werden.
- **Auf Client zu verwendender minimal verfügbarer Bandbreitenprozentsatz:** Legt den Umfang der dynamischen Bandbreitendrosselung fest. Sie können Werte bis zu 50 Prozent der für einen Client verfügbaren Gesamtnetzwerkbandbreite angeben. Wenn beispielsweise während der Verteilung eine andere Anwendung auf dem Client Netzwerkbrandbreite nutzt und Sie den Brandbreitenprozentsatz 50 Prozent angeben, dann erhält der Verteilungsauftrag 50 Prozent und die Clientanwendung ebenfalls 50 Prozent. In der Praxis ist diese Prozentangabe variabel, weil das Betriebssystem automatisch einen Großteil der Netzwerkbandbreite abhängig von der Anzahl und der Priorität der Anwendungen zuweist, die Netzwerkbandbreite benötigen.
- **Verzögerung zwischen Paketen (Peer):** Diese Option legt die Verzögerung zwischen Paketen fest, die an Peers im gleichen Subnetz gesendet werden. Sie können Verteilungen mithilfe dieser Verzögerung beschleunigen und verlangsamen. Wenn die Verzögerung zwischen Paketen erhöht wird, dann erfolgt die Verteilung langsamer und unter geringem Einsatz von Bandbreite. Sie können diese Option zusammen mit der Option **Dynamische Bandbreitendrosselung** verwenden. Wenn Sie dies tun, fällt die Paketverzögerung jedoch stärker ins Gewicht.

- **Verzögerung zwischen Paketen (Quelle):**Legt die Verzögerung zwischen der Paketquelle und dem Zielclient fest. Wenn die Verzögerung zwischen Paketen erhöht wird, dann erfolgt die Verteilung langsamer und unter geringem Einsatz von Bandbreite. Sie können diese Option zusammen mit der Option **Dynamische Bandbreitendrosselung** verwenden. Wenn Sie dies tun, fällt die Paketverzögerung jedoch stärker ins Gewicht.

Infos über die Seite "Auftragsoptionen"

Auf dieser Seite konfigurieren Sie, wie die betreffende Verteilung bereitgestellt wird. Wenn Sie eine MSI-Datei oder eine generische ausführbare Datei verteilen, haben Sie die Option, beliebige Befehlszeilenparameter einzugeben, die nach dem Multicast an die Datei weitergegeben werden müssen.

- **Skript verwendet Standard-Distributionslimit:** Sie können die Zahl der Computer begrenzen, auf die Targeted Multicast die gleichzeitige Verteilung vornimmt. Diese Option verwendet den Standardwert, den Sie im Dialogfeld **Management Suite-Dienste konfigurieren** auf der Registerkarte **Benutzerdefinierte Aufträge** unter **Verteilen an X Computer gleichzeitig** festgelegt haben.
- **Skript verwendet benutzerdefiniertes Distributionslimit:** Verwenden Sie diese Option, um den Standard für den aktuellen Auftrag durch Festlegen eines anderen Werts zu überschreiben.
- **Nur vom Cache oder Peer installieren:** Durch diese Option werden Zielcomputer daran gehindert, ihr Subnetz für die Installation eines Pakets zu überschreiten. Computer suchen zuerst in ihrem Multicast-Cacheverzeichnis. Wenn das Paket dort nicht vorhanden ist, führen sie die Prüfung auf Pakete mit Peers auf ihrem Subnetz durch. Wenn keiner der Peers das Paket besitzt, schlägt die Verteilung fehl. Diese Option minimiert den Netzwerkverkehr innerhalb von Subnetzen. Sie können diese Option verwenden, nachdem Sie ein Paket auf jedes Subnetz über die Seite "Skript erstellen" mit der Option **Nur Dateien auf dem Computer cachen, die Multicast verwenden** kopiert haben.
- **Datei vor Client-Installation überprüfen:** Erzeugt eine Prüfsumme (CRC) für das zu verteilende Paket, sobald der Asssistent beendet wird. Clients können mithilfe dieses Prüfsummenwerts sicherstellen, dass die empfangene Datei/das Paket nicht beschädigt ist. Abhängig von der Größe der zu verteilenden Datei bzw. des Pakets, kann die Berechnung der Prüfsumme einige Minuten in Anspruch nehmen.
- **Befehlszeileneintrag für MSI-Pakete oder generische EXE:** Diese Option wird nur dann angezeigt, wenn Sie ein MSI-Paket verteilen. Sie können hier Befehlszeilenoptionen für das MSI-Paket eingeben.

Infos über die Seite "Feedback-Optionen"

Verwenden Sie diese Seite, um zu entscheiden, wie viel dem Benutzer während der Installation oder der Deinstallation der Software angezeigt wird. Die folgenden Optionen stehen Ihnen zur Verfügung:

- **Kein Feedback anzeigen:** Diese Option verbirgt die Installation gegenüber dem Benutzer in dem Maße, wie es die Softwareverteilungspakete erlauben. Wenn Sie das Softwareverteilungspaket als "still" erstellt haben, gewährleistet diese Option, dass es still installiert wird. Wenn das Softwareverteilungspaket mit Benutzerinteraktion erstellt wurde, kann diese Option nicht garantieren, dass sämtliche Benutzerinteraktion vermieden wird.
- **Installations-/Entfernungsverlauf für Benutzer anzeigen:** Diese Option ermöglicht Ihnen die Auswahl einer der folgenden Möglichkeiten:
  - **Hintergrundbildschirm anzeigen:** Diese Option steuert, ob der vollständige Hintergrundbildschirm, der den Desktop verbirgt, während des Vorgangs angezeigt wird.
  - **Benutzer darf abbrechen:** Diese Option ermöglicht es dem Benutzer, die Aktion abzubrechen: entweder eine Installation oder die Deinstallation. Diese Option wird nicht für Anwendungsrichtlinien empfohlen.

Festlegen des Feedbacks für andere Pakettypen

Verwenden Sie die Feedback-Optionen, um zu entscheiden, wie viel dem Benutzer während der Installation oder der Deinstallation der Software angezeigt wird. Bei MSI-Paketen, Paketen, die mit früheren Versionen von Management Suite erstellt wurden und bei generischen ausführbaren Dateien haben Sie zwei Optionen. Die internen Einstellungen dieser Pakete können jedoch dazu führen, dass die Benutzeroberfläche unabhängig von diesen Einstellungen generiert wird.

- **Kein Feedback anzeigen:** Diese Option verbirgt die Installation gegenüber dem Benutzer in dem Maße, wie es das Paket erlaubt. Wenn Sie das Paket als "still" erstellt haben, gewährleistet diese Option, dass es still ist. Wenn das Paket mit Benutzerinteraktion erstellt wurde, kann diese Option nicht garantieren, dass sämtliche Benutzerinteraktion vermieden wird.
- **Installations-/Entfernungsverlauf für Benutzer anzeigen:** Diese Option ermöglicht Ihnen die Auswahl einer der folgenden Möglichkeiten:
  - **Benutzer darf abbrechen:** Diese Option ermöglicht es dem Benutzer, die Aktion abzubrechen: entweder eine Installation oder die Deinstallation. Diese Option wird nicht für Anwendungsrichtlinien empfohlen.
  - **Vollständige Paket-Benutzeroberfläche anzeigen** Diese Option steuert, ob der vollständige Hintergrundbildschirm, der den Desktop verbirgt, während des Vorgangs angezeigt wird.

Info über die Seite "Neuinstallations- und Reparaturoptionen"

Auf dieser Seite legen Sie fest, welche Aktion erfolgt, wenn Anwendungen bereits auf den Clients installiert sind. Wenn Anwendungen vorhanden sind, die nicht auf eine normale Paketreparatur reagieren, ist die Option für eine komplette Neuinstallation möglicherweise besser geeignet. Reparaturen erfordern in der Regel weniger Zeit als eine komplette Neuinstallation.

- **Das Paket reparieren:** Durch diese Option werden die Registrierungsschlüssel nur aktualisiert und nur die Programmdateien, die der Agent als abweichend von den Dateien im Installationspaket erkennt, ersetzt.

- **Das Paket komplett neu installieren:** Durch diese Option wird das Paket komplett neu installiert, alle Dateien ersetzt und alle Registrierungsschlüssel neu erstellt.
- **Benutzer darf entscheiden, ob repariert oder neu installiert wird:** Diese Option fordert den Benutzer zur Eingabe auf, welchen Typ der Installation er durchführen möchte.

Infos über die Seite "Neustartoptionen"

Auf dieser Seite legen Sie fest, ob der Computer neu gestartet wird, nachdem die Software installiert oder deinstalliert wurde. Es stehen Ihnen drei Optionen zur Verfügung:

- **Nie neu starten:** Clients werden nach einer Paketinstallation nicht neu gestartet. Wenn Sie diese Einstellung wählen und das Paket einen Neustart erfordert, kann es auf den Clients zu Fehlern bei der Anwendungsausführung kommen, sofern kein Neustart durchgeführt wird. Wenn es sich bei dem Paket um ein ESWD-Paket handelt, überschreibt diese Option alle Einstellungen im Paket. Wenn es sich bei dem Paket um eine generische ausführbare Datei oder um ein MSI-Paket handelt, überschreibt die Paketeinstellung möglicherweise diese Option.
- **Nur bei Bedarf neu starten:** Clients werden neu gestartet, wenn es das Paket erfordert.
- **Immer neu starten:** Clients werden neu gestartet, unabhängig davon, ob es das Paket erfordert oder nicht.

Infos über die Seite "Bereitstellungszeitoptionen"

Über diese Seite können Sie steuern, wann das Paket verteilt wird, nachdem es beim Client angekommen ist. Sie müssen keine dieser Optionen auswählen, wenn Sie möchten, dass das Paket installiert wird, sobald Sie es geplant haben. Vergewissern Sie sich, bevor Sie diese Optionen verwenden, dass Sie den Local Scheduler-Agenten auf den Clients installiert haben.

Wenn Sie den Clients einen Teil der Steuerung überlassen möchten, haben Sie zwei Optionen:

- **Installation/Deinstallation bis zur nächsten Benutzeranmeldung verzögern:** Diese Option verzögert die Installation, bis sich das nächste Mal ein Benutzer am Computer anmeldet.
- **Benutzer darf Task verzögern:** Diese Option ermöglicht es dem Benutzer, die Aktion zu verzögern. Sie können diese Option anpassen, indem Sie Folgendes konfigurieren:
- **Benutzerdefinierte Verzögerungsmeldung angeben:** Wenn Sie diese Option aktivieren, können Sie eine benutzerdefinierte Verzögerungsmeldung angeben.
- **Verzögerungstimeout in Sekunden:** Mit dieser Option können Sie angeben, wie lange gewartet wird, bis der Benutzer eine Verzögerungszeit eingibt. Die Standardwartezeit beträgt 60 Sekunden. Wenn der Benutzer nicht auf die Anforderung zur Eingabe einer Verzögerungszeit innerhalb der festgelegten Zeit reagiert, wird mit der Installation begonnen.

Infos über die Seite "Bandbreitenoptionen"

Über diese Seite können Sie die Netzwerkbandbreite steuern, die das Paket für die Verteilung erfordert. Sie müssen keine dieser Optionen auswählen, wenn Sie möchten, dass alle gewählten Clients das Paket unabhängig von ihrer Bandbreite erhalten.

Die Bandbreitensteuerung ist wichtig für Clients mit einer langsamen WAN- oder Einwahlverbindung. In der Regel werden Sie keine Installationen von Multimegabytepaketen auf Clients mit langsamen Verbindungen vornehmen. Wählen Sie eine der folgenden Optionen aus:

- **Eine Nicht-RAS-Netzwerkverbindung erfordern:** Diese Option aktiviert die Bandbreitenvoraussetzung. Wählen Sie eine der folgenden Optionen:
    - **Alle Nicht-RAS-Netzwerkverbindungen zulassen:** Diese Option aktiviert WAN- und LAN-Clients für den Empfang des Pakets:
    - **Nur Hochgeschwindigkeitsverbindung zulassen:** Diese Option aktiviert nur LAN-Clients für den Empfang des Pakets.

Wenn Sie PDS zum Erkennen der Netzwerkgeschwindigkeit verwenden, geben Hochgeschwindigkeits- und langsame Verbindungen dieselben Daten zurück. Sie müssen ICMP verwenden, damit Hochgeschwindigkeits-Netzwerkverbindungen richtig erkannt werden.

ICMP sendet ICMP-Echoanforderungen verschiedener Größe an die Ferncomputer und verwendet das Antwortverhalten dieser Echoanforderungen bzw. -reaktionen, um die ungefähre Bandbreite zu bestimmen. Allerdings unterstützen nicht alle Router oder Computer das Weiterleiten oder Beantworten von ICMP-Echoanforderungen. ICMP unterscheidet auch zwischen LAN (Hochgeschwindigkeits-) und WAN (langsame, jedoch keine Einwahl-) Verbindungen.

Wenn das Netzwerk nicht für das Zulassen von ICMP-Echoanforderungen konfiguriert ist, können Sie PDS wählen. Wenn Sie PDS verwenden, erhalten Sie über die Option "Nur Hochgeschwindigkeitsverbindung zulassen" keine genaue Steuerung.

Infos über die Seite "Fertig"

Diese Seite fasst die Aktionen zusammen, die Sie für die Installation des Pakets ausgewählt haben. Vergewissern Sie sich vor dem Fortfahren, dass die Clients alle Voraussetzungen erfüllen, die im Warnabschnitt aufgeführt sind.

Wenn Sie auf **Als Standard festlegen** klicken, werden die ausgewählten Konfigurationsoptionen als Standardwerte für den Paketbereitstellungsassistenten festgelegt.

Klicken Sie auf **Fertigstellen** und der Assistent gibt im Fenster "Geplante Tasks" zurück, ob Sie ein Softwareverteilungsskript erstellen bzw. im Fenster "Application Policy Manager", ob Sie eine Anwendungsrichtlinie erstellen. In diesen Fenstern können Sie Ziele für die Paketverteilung hinzufügen.

Info über die Seite "Multicast-Optionen"

Im Fenster "Multicast-Optionen" des Assistenten für das Erstellen von Verteilungspaketskripts können Sie auftragsspezifische Targeted Multicast-Parameter konfigurieren. Die Standardwerte in diesem Dialogfeld sind in der Regel für die meisten Multicasts geeignet. Auswirkungen der Optionen:

- **Höchstzahl gleichzeitig arbeitender Multicast-Domänenrepräsentanten:** Die Zahl der Repräsentanten, die aktiv zur selben Zeit einen Multicast durchführen, ist auf diese Anzahl beschränkt.
- **Verarbeitung von Rechnern einschränken, bei denen Multicast fehlschlug ...:** Wenn ein Client die Datei über Multicast nicht erhält, wird sie aus dem Web oder vom Dateiserver heruntergeladen. Dieser Parameter kann verwendet werden, um die Anzahl der Clients zu beschränken, die die Datei gleichzeitig erhalten. Wenn z.B. die Höchstanzahl von Threads 200 war und die Höchstanzahl der fehlgeschlagenen Multicast-Threads bei 20 lag, würden im Dialogfeld "Benutzerdefinierte Aufträge" nicht mehr als 20 Computer gleichzeitig verarbeitet werden, bei denen Multicast fehlgeschlagen ist. Das Dialogfeld "Benutzerdefinierte Aufträge" verarbeitet bis 200 Clients gleichzeitig, wenn sie erfolgreich den Multicast erhalten haben. Es verarbeiten jedoch nicht mehr als 20 der 200 Threads Clients, bei denen der Multicast-Task fehlgeschlagen ist. Wenn dieser Wert auf 0 festgelegt ist, führt das Dialogfeld "Benutzerdefinierte Aufträge" den Verteilungsabschnitt des Task für keinen der Computer durch, auf dem das Multicasting fehlgeschlagen ist.
- **Anzahl von Tagen, die die Dateien im Cache des Clients verbleiben:** Die Zeit, die die Datei, für das Multicasting durchgeführt wird, im Cache auf den einzelnen Zielcomputern bleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Anzahl von Tagen, die die Dateien im Cache des Multicast-Domänenrepräsentanten verbleiben:** Die Zeitspanne, über die die Datei, für das Multicasting durchgeführt wird, im Cache auf dem Multicast-Domänenrepräsentanten verbleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Minimale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Mindestwartezeit zwischen dem Senden von Multicast-Paketen. Dieser Wert wird nur verwendet, wenn der Repräsentant kein Multicasting einer Datei aus dem eigenen Cache durchführt. Wenn dieser Parameter nicht festgelegt wird, wird die auf dem Subnetz/Domänenrepräsentantencomputer gespeicherte Mindestruhezeit verwendet. Sie können mithilfe dieses Parameters die Bandbreitennutzung im WAN beschränken.
- **Maximale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Höchstwartezeit zwischen dem Senden von Multicast-Paketen. Weitere Informationen finden Sie weiter oben unter "Mindestzahl in Millisekunden zwischen Paketübertragungen".
- **Wartezeit in Sekunden nach Wake on LAN:** Legt fest, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das Wake On LAN-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden. Wenn Computer im Netzwerk länger als 120 Sekunden zum Starten benötigen, sollten Sie diesen Wert erhöhen. Der zulässige Höchstwert liegt bei 3600 Sekunden (eine Stunde).

Info über das Dialogfeld "Benutzerdefiniertes Skript erstellen"

Mithilfe dieser Seite können Sie ein benutzerdefiniertes Skript erstellen. Sobald Sie einen Skriptnamen eingegeben und auf "OK" geklickt haben, wird das Skript in Notepad geöffnet, damit Sie es bearbeiten können. Weitere Informationen zur Skripterstellung finden Sie im Skript-Handbuch für .CFG-Dateien weiter oben in diesem Kapitel.

Info über die Assistentenseite "Anwendungsrichtlinie erstellen"

Legen Sie auf der Assistentenseite "Anwendungsrichtlinie erstellen" den Namen der Richtlinie fest, die Sie konfigurieren und ob diese Richtlinie installiert oder deinstalliert werden soll.

- **Anwendungsrichtlinienname:** Geben Sie den Namen der Anwendung ein, die Sie konfigurieren. Dieser Name wird in der Spalte "Anwendungsreparaturliste" angezeigt.
- **Installieren:** Wählen Sie diese Option, um die Richtlinie auf Clients zu erstellen.
- **Deinstallieren:** Wählen Sie diese Option, um die Richtlinie von Clients zu deinstallieren.

Info zum Handheld Manager

LANDesk Handheld Manager ist ein Add-on für LANDesk Management Suite 8, mit dessen Hilfe Sie mobile Geräte verwalten können. LANDesk Software, Inc. hat eine Partnerschaft mit XcelleNet Afaria* geschlossen, um die Unterstützung für die mobile Verwaltung zu ermöglichen. Mithilfe von Handheld Manager senden Ihre mobilen Geräte Inventardaten an die Core-Datenbank von Management Suite. Außerdem können Sie mit Handheld Manager einzelne Dateien oder Einzeldateipakete (gilt nur für 32-Bit-Windows-Plattformen) auf Ihren mobilen Geräten verteilen.

Handheld Manager muss auf Ihrem Management Suite 8-Core Server installiert werden. Der Afaria-Agent muss auf allen mobilen Geräten installiert werden, die verteilte Pakete erhalten sollen.

Weitere Informationen finden Sie in der Dokumentation auf der Handheld Manager-CD.

So verteilen Sie Pakete über Handheld Manager

1. Erstellen Sie das Paket, das Sie verteilen möchten. Klicken Sie auf **Extras | Verteilungspaketskript erstellen** und wählen Sie die Datei für die Verteilung aus. Klicken Sie im Paketbereitstellungsassistenten auf **Paket mit Mobile Manager bereitstellen**. Beenden Sie den Assistenten.
2. Planen Sie einen Auftrag von der Konsole aus, um das Paket auf die mobilen Geräte zu verteilen.
3. Wenn der geplante Zeitpunkt eingetreten ist, startet der Scheduler den mobilen Taskprozessor (LDHTASK.EXE), um den Task zu verarbeiten.
4. Nachdem LDHTASK.EXE gestartet wurde, überträgt sie die Datei von ihrem ursprünglichen Speicherort, die Sie im Verzeichnis der Handhelddateien auf dem Core Server angegeben haben.

5. Sobald sich die Datei im Verzeichnis befindet, werden die mobilen Geräte, die Teil des geplanten Task sind, als bereit für die Verarbeitung in der Core-Datenbank gekennzeichnet. Dieser Task bleibt im Fenster "Geplante Tasks", bis die Zielclients den Task abgeschlossen haben.
6. Wenn ein mobiles Gerät den Core Server das nächste Mal über den Afaria-Agenten kontaktiert, prüft das Gerät, ob für seine eindeutige Geräte-ID Tasks geplant sind. Wenn für das Gerät ein Task geplant ist, ruft der Afaria-Agent die geplante Datei ab und installiert sie. Management Suite empfängt den Auftragsstatus vom Afaria-Agenten. Statusmeldungen werden im Fenster "Geplante Tasks" angezeigt.

Info über das Statusfenster "Multicast Software Distribution"

Dieses Fenster wird angezeigt, wenn eine aktive Verteilung über Targeted Multicast durchgeführt wird. In diesem Fenster werden die folgenden Informationen angezeigt:

- **Paket-URL oder UNC-Pfad:** Dies ist der Speicherort des Pakets, das Sie gegenwärtig verteilen möchten.
- **Status:** Ein Echtzeitbericht über das Fortschreiten der Verteilung bzw. über den Erfolg des abgeschlossenen Auftrags.
- **Multicast-Domänen:** Das Feld oben zeigt alle Subnetze und die Multicast-Domänenrepräsentanten, die bei der Verteilung verwendet werden. Wenn Sie jeden Domänenrepräsentanten markieren, zeigt das untere Fenster alle Computer an, die ihre Verteilung von diesem Domänenrepräsentanten erhalten.
  Jeder Computer im unteren Fenster zeigt Informationen über den Abschluss der Verteilung auf diesem Computer an. Es gibt mehrere Informationsfelder auf der rechten Seite der aufgeführten Computer, einschließlich Felder über nicht erhaltene Pakete, Neusendungsanforderungen und zum Verlangsamen von Anforderungen. Diese Felder enthalten erst Informationen, wenn die Verteilung abgeschlossen ist.
- **Nicht erhaltene Pakete:**Zeigt die Zahl der Pakete an, die der Client nicht vom Subnetzrepräsentanten empfangen konnte. Wenn die Zahl ungleich 0 war, ist die Verteilung fehlgeschlagen.
- **Anforderungen erneut senden:**Zeigt an, wie oft der Client dieses Paket für die Neusendung vom Subnetzrepräsentanten anfordern musste. Dies ist eine gute Methode, um abzuschätzen, wie beschäftigt der Client war mit der Handhabung von anderen Vorgängen während der Verteilung.
- **Anforderungen verlangsamen:**Zeigt an, wie oft der Client die Anforderung nach einem Verlangsamen des Paketstroms anfordern musste. In diesem Fall zeigen hohe Zahlen in der Regel an, dass beim Computer Hardwareprobleme vorliegen, die die Verteilung verlangsamen. Wenn Sie viele Computer mit einer Anforderung nach einer Verlangsamung haben, sollten Sie die Verzögerungs-/Paketnummer auf dem Subnetzrepräsentanten prüfen. Häufig liegt ein Zusammenhang zwischen der Verzögerungs-/Paketnummer und der Zahl der Anforderungen nach einem Verlangsamen vor.

Das Fenster wird automatisch nach 10 Sekunden geschlossen. Wenn das Fenster während der gesamten Verteilung geöffnet bleiben soll, klicken Sie auf **Dialogfeld geöffnet lassen**. Das Fenster bleibt geöffnet, bis Sie es manuell schließen. Wenn dieses Dialogfeld geöffnet bleibt, wird die Skriptausführung beendet. Daher müssen Sie darauf achten, dass Sie das Dialogfeld schließen.